Travail d'études et de recherche

Institut Fourier
Université Grenoble Alpes

Réalisabilité de Groupes

Mathis Alleysson
encadré par
Rémi Molinier

12 mai 2022

Table des matières

I Éléments de théorie des catégories 2
I.1 Définitions . . . 2
I.2 Automorphismes . . . 4

II Groupes 5

III Graphes finis 8
III.1 Définitions et cadre . . . 8
III.2 Quelques exemples et propriétés . . . 12
III.2.1 Graphe image . . . 12
III.2.2 Graphes complets . . . 13
III.2.3 Graphes connexes . . . 14
III.3 Graphe de Cayley . . . 16
III.4 Automorphisme préservant la couleur . . . 18
III.5 Extension au cas non orienté . . . 21

IV Ordinaux 25
IV.1 Relations et propriétés . . . 25
IV.2 Ordre . . . 26
IV.3 Catégorie sur les ordres . . . 27
IV.4 Opérations sur les ordres . . . 29
IV.5 Ordinaux . . . 30
IV.6 Arithmétique ordinale . . . 35
IV.7 Equipotents . . . 36

V Graphes infini 38

VI Corps 47
VI.1 Les extensions de $\mathbb{Q}$ en tant que catégorie . . . 47
VI.2 Notions de théorie de Galois . . . 48
VI.3 Réalisabilité sur la catégorie des extensions de $\mathbb{Q}$ . . . 53

VII Espaces topologiques 58

VIII Foncteurs & Conclusion 61
VIII.1 Foncteurs . . . 61
VIII.2 Tableau résumé . . . 62

Références 63

Introduction

Soit $\mathcal{C}$ une catégorie (nous préciserons cela dès la prochaine section). Pour tout élément A de $\mathcal{C}$ il est possible de définir un groupe d'automorphismes associé à cet élément (noté $\mathrm{Aut}_{\mathcal{C}}(A)$), celui-ci contient grossièrement les transformations bijectives de A dans lui-même, qui préserve la structure associée à la catégorie $\mathcal{C}$. L'objectif de la réalisabilité de groupe (et donc de ce travail d'études et de recherche) est de déterminer des catégories $\mathcal{C}$ qui vérifient le problème de "Réalisabilité" qui est le suivant :

Pour tout groupe G, existe-t-il un élément A de $\mathcal{C}$ tel que $\mathrm{Aut}_{\mathcal{C}}(A)$ soit un groupe isomorphe à G ?

Le premier exemple de catégorie auquel nous pouvons penser est la catégorie des groupes. Malheureusement, nous prouverons en étudiant l'exemple de $\mathbb{Z}/3\mathbb{Z}$, que dans cette catégorie, il n'est pas possible de réaliser tout groupe. Pour trouver notre premier exemple de réalisabilité de groupes, nous devrons étudier la catégorie des graphes. En effet, Robert Wertheimer Frucht a montré que la catégorie des graphes non orientés réalise tous les groupes, en utilisant une autre construction de graphe : le graphe de Cayley. Le théorème de Frucht est la brique principale de l'étude de la réalisabilité de groupe d'autres catégories, il est en effet possible de montrer que la catégorie des extensions de corps de $\mathbb{Q}$ ou, que la catégorie des espaces topologiques réalise tous les groupes, en se basant sur le Théorème de Fruch et c'est ce que nous étudierons aussi dans la suite.

I Éléments de théorie des catégories

I.1 Définitions

Afin de correctement définir le problème, il nous faut un peu préciser les objets avec lesquels nous travaillerons.

Definition I.1.1 (Catégorie) Une *catégorie* $\mathcal{C}$ est la donnée de :

- Une classe $\mathrm{ob}(\mathcal{C})$ dont les éléments sont appelés : *objets* de la catégorie.
- Une classe $\mathrm{mor}(\mathcal{C})$ dont les éléments sont appelés : *morphismes* de la catégorie.
- $\mathcal{S}, \mathcal{B}$ deux applications de $\mathrm{mor}(\mathcal{C})$ dans $\mathrm{ob}(\mathcal{C})$ que l'on nomme *source* et *but*. Pour tout morphisme f on notera donc $f : \mathcal{S}(f) \to \mathcal{B}(f)$ et si A, B sont deux objets alors on note $\mathrm{Hom}_{\mathcal{C}}(A, B)$ la classe de tous les morphismes $f : A \to B$.
- Pour tout objet A, un morphisme $id_A : A \to A$, appelé l'identité de A.
- Une composition $\circ$ telle que si $f : A \to B$ et $g : B \to C$ sont deux morphismes, alors $g \circ f : A \to C$ est un morphisme appelé *composé* de f et g et on a de plus les propriétés :
  - Pour tous morphismes $f : A \to B$, $g : B \to C$ et $h : C \to D$, on a $(h \circ g) \circ f = h \circ (g \circ f)$.
  - Pour tous morphisme $f : A \to B$, on a $id_B \circ f = f = f \circ id_A$.

Definitions I.1.2 Soit $\mathcal{C}$ une catégorie.

— On dit que $\mathcal{C}$ est *localement petite* si, pour tous objets A,B de $\mathcal{C}$, la classe des morphismes de A dans B, i.e. $\mathrm{Hom}_{\mathcal{C}}(A, B)$ est un ensemble.

— On dit que $\mathcal{C}$ est *petite* si la classe des morphismes de $\mathcal{C}$, i.e. $\mathrm{mor}(\mathcal{C})$ est un ensemble.

Definition I.1.3 Soit $\mathcal{C}$ une catégorie. Une *sous-catégorie* $\mathcal{B}$ de $\mathcal{C}$ est une catégorie telle que :

— $\mathrm{ob}(\mathcal{B})$ est une sous-classe de $\mathrm{ob}(\mathcal{C})$.

— Pour tous $A, B \in \mathrm{ob}(\mathcal{B}) \subset \mathrm{ob}(\mathcal{C})$, $\mathrm{Hom}_{\mathcal{B}}(A, B)$ est une sous-classe de $\mathrm{Hom}_{\mathcal{C}}(A, B)$

— La composition de $\mathcal{B}$ est définie comme sur $\mathcal{C}$: Si on prend $f : A \to B$ et $g : B \to C$ deux morphismes de $\mathcal{B}$, en notant $h = g \circ f$ la composée dans, $\mathcal{C}$ on obtient que $h \in \mathrm{Hom}_{\mathcal{B}}(A, C)$ et h est la composée de f et g aussi dans $\mathcal{B}$.

Remarque: La notion de "classe" et "application" doit être maniée minutieusement, nous ne nous intéresserons pas à ces problèmes ici, mais l'on pourra par exemple regarder la source [8] ou l'article `https://en.wikipedia.org/wiki/Von_Neumann%E2%80%93Bernays%E2%80%93G%C3%B6del_set_theory`.

Caractérisons un peu plus certains morphismes avec les définitions suivantes.

Definitions I.1.4 Soit $\mathcal{C}$ une catégorie et A, B deux éléments de $\mathcal{C}$. Soit $f : A \to B$ un morphisme.

— On dit que f est un *monomorphisme* s'il vérifie la propriété suivante : pour tout E élément de $\mathcal{C}$ et pour tous $g, h : E \to A$ si on a $f \circ g = f \circ h$, alors $g = h$.

— On dit que f est un *épimorphisme* s'il vérifie la propriété suivante : pour tout E élément de $\mathcal{C}$ et pour tous $g, h : B \to E$ si on a $g \circ f = h \circ f$, alors $g = h$.

Exemple (Catégorie Set): Avec la classe de tous les ensembles, on peut définir une catégorie que l'on notera Set. En effet, pour cela on dit que $\mathrm{ob}(Set)$ est la classe de tous les ensembles (notés par exemple $A, B, C, ...$), $\mathrm{mor}(Set)$ est la classe de toutes les applications (au sens usuel, notées par exemple $A \to B$) d'un ensemble dans un autre ensemble, la source est l'application qui à une application entre ensembles renvoie l'ensemble de définition (dans notre exemple, c'est A), le but est l'application qui à un morphisme renvoie l'ensemble d'arrivée (toujours dans notre exemple, c'est B), la loi de composition est la composition d'applications entre ensembles, par exemple si $f : A \to B$ et $g : B \to C$ sont deux applications alors $g \circ f : A \to C$ est définie par : pour tout $x \in A, (g \circ f)(x) = g(f(x))$ et finalement pour tout ensemble A on définit l'identité par :

$$id_A : \begin{array}{ccc} A & \to & A \\ x & \mapsto & x \end{array}$$

De plus pour la catégorie Set les monomorphismes sont les applications injectives, les épimorphismes sont les applications surjectives et les morphismes qui sont à la fois des monomorphismes et des épimorphismes sont les bijections. Dans la suite, nous ne considérerons pas la catégorie Set mais des sous-catégories de Set auquel on

ajoute de la structure, par exemple la catégorie des groupes (notée Grp). L'intérêt d'étudier des sous-catégories de Set c'est que celles-ci ont pour classe de morphismes une sous-classe des morphismes de Set (qui sont, pour rappel, les applications entre ensemble), et donc comme Set est une catégorie localement petite, on obtient que ces autres catégories sont aussi localement petites.

I.2 Automorphismes

Definition I.2.1 (Isomorphismes) Soit $\mathcal{C}$ une catégorie. On notera $\circ$, la loi de composition associée. Soient A, B deux éléments de $\mathcal{C}$ et $f : A \to B$ un morphisme de $\mathcal{C}$. On dit que f est un *isomorphisme* de $\mathcal{C}$ s'il existe $g : B \to A$ un morphisme de $\mathcal{C}$ tel que :

$$f \circ g = id_B, \quad g \circ f = id_A$$

On appelle g l'*inverse* de f et on le note généralement f^{-1}.

Remarque: Un isomorphisme est un monomorphisme et un épimorphisme, mais la réciproque est vraie pour Set mais fausse en général. Par exemple, si l'on considère la catégorie des anneaux munis des morphismes d'anneaux (que nous définirons plus tard, voir : VI.1.4) alors on sait que les morphismes $\mathbb{Z} \to \mathbb{Q}$ sont parfaitement déterminés par l'image de 1 (car $\langle 1 \rangle = \mathbb{Z}$ et les éléments de $\mathbb{Q}$ sont des quotients d'éléments de $\mathbb{Z}$, donc parfaitement déterminé). On peut voir que l'inclusion :

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Q} \\ x & \mapsto & x \end{array}$$

est un épimorphisme et un monomorphisme, mais n'est pas surjectif, donc n'est pas un isomorphisme, car dans la catégorie des morphismes d'anneaux un isomorphisme est en particulier bijectif.

Definition I.2.2 (Automorphismes) Soit $\mathcal{C}$ une catégorie. Soit $A \in \mathcal{C}$. On définit la *classe des automorphismes* de A comme étant la classe de tous les morphismes $A \to A$ qui sont aussi des isomorphismes de $\mathcal{C}$. On la notera
$Aut_{\mathcal{C}}(A)$.

Remarque: Si $\mathcal{C}$ est une catégorie localement petite et $A \in \mathcal{C}$, on nommera plutôt la classe des automorphismes comme l'*ensemble des automorphismes*, car c'est une sous-classe de $\mathrm{Hom}_{\mathcal{C}}(A, A)$ qui est un ensemble.

Nous allons donc dans la suite étudier l'ensemble des automorphismes d'une catégorie localement petite. Pour commencer, montrons que cet ensemble peut être muni d'une structure de groupe.

Definitions I.2.3 (Groupe) Soit G un ensemble.

— Une *loi de composition interne* sur G est une application qui, à deux éléments de G associe un élément de G.

$$G \times G \to G$$

— Soit $\bullet$ une loi de composition interne sur G, on dit que $(G, \bullet)$ est un *groupe* si on vérifie :

(i) $\bullet$ est associative : $\forall x, y, z \in G, x \bullet (y \bullet z) = (x \bullet y) \bullet z$,

(ii) $\bullet$ admet un neutre : $\exists 1_G \in G, \forall x \in G, x \bullet 1_G = x = 1_G \bullet x$,

(iii) tout élément admet un inverse : $\forall x \in G, \exists! y \in G, x \bullet y = y \bullet x = 1_G$.

En général, si $(G, \bullet)$ est un groupe, on le notera simplement G et on oubliera parfois de préciser la loi dans les énoncés et calculs suivants s'il n'y a pas d'ambiguïté.

On dit qu'un groupe G est dit *abélien* s'il est *commutatif*, c'est-à-dire : $\forall x, y \in G, xy = yx$.

Propriété I.2.4 *Soit $\mathcal{C}$ une catégorie localement petite et $\circ$ la composition associée à $\mathcal{C}$. Soit A un élément de $\mathcal{C}$. On peut définir sur $\mathrm{Aut}_{\mathcal{C}}(A)$ une structure de groupe grâce à la composition de $\mathcal{C}$.*

Preuve. Tout d'abord, $\mathcal{C}$ étant localement petite, on obtient que :

$$\mathrm{Aut}_{\mathcal{C}}(A) \subset \mathrm{Hom}_{\mathcal{C}}(A, A),$$

est un ensemble. De plus, par définition de catégorie, on obtient que $\circ$ est une loi de composition interne, associative sur les morphismes de $\mathcal{C}$.

Soient $f, g : A \to A$ deux éléments de $\mathrm{Aut}_{\mathcal{C}}(A)$. $\circ$ étant une loi de composition interne on a déjà que $f \circ g$ est un morphisme de $\mathcal{C}$, de plus si on note f^{-1} et g^{-1} les inverses de f et g alors on a :

$$(f \circ g) \circ (g^{-1} \circ f^{-1}) = id_A = (g^{-1} \circ f^{-1}) \circ (f \circ g),$$

donc $g^{-1} \circ f^{-1}$ est l'inverse de $f \circ g$, ainsi $f \circ g$ est un isomorphisme de $\mathcal{C}$ et un morphisme $A \to A$, donc $f \circ g \in \mathrm{Aut}_{\mathcal{C}}(A)$ et finalement $\circ$ est une loi de composition interne sur $\mathrm{Aut}_{\mathcal{C}}(A)$.

L'associativité de $\circ$ sur $\mathrm{Aut}_{\mathcal{C}}(A)$ découle de celle sur $\mathcal{C}$.

On a également que id_A est un neutre pour notre groupe. En effet, par définition de catégorie, on a que pour tout morphisme $f : A \to B$, $id_B \circ f = f = f \circ id_A$. De plus $id_A \in \mathrm{Aut}_{\mathcal{C}}(A)$ et son inverse est lui-même.

Finalement, comme tout élément de $\mathrm{Aut}_{\mathcal{C}}(A)$ est un isomorphisme, il admet un inverse. Donc $(\mathrm{Aut}_{\mathcal{C}}(A), \circ)$ est un groupe. □

II Groupes

La première catégorie que nous pouvons étudier et celle des groupes Grp qui sont définis dans la Définition I.2.3. Pour cela, commençons par définir les morphismes de cette catégorie :

Definition II.0.1 Soient $(G, \bullet)$, $(H, *)$ deux groupes et $f : G \to H$ une application. On dit que f est un *morphisme de groupes* si :

$$\forall (x, y) \in G^2, f(x \bullet y) = f(x) * f(y)$$

La définition d'isomorphisme est héritée de celle sur Ens ainsi que la composition. Donc,on peut définir l'ensemble des automorphismes de groupes d'un groupe G. On le notera $\mathrm{Aut}_{Grp}(G)$. La question de la réalisabilité de groupes de Grp se résout avec l'énoncé suivant :

Proposition II.0.2 *Il n'existe pas de groupe tel que son groupe d'automorphisme soit isomorphe à* $\mathbb{Z}/3\mathbb{Z}$.

Avant de passer à la preuve, il nous faut travailler un peu.

Definitions II.0.3 Soit G un groupe.

— Le *centre* de G est : $\mathrm{Z}(G) := \{x \in G \mid \forall g \in G, gx = xg\}$

— Le groupe des *automorphismes intérieurs* est :

$$\mathrm{Inn}(G) := \left\{ i_g : \begin{array}{ccc} G & \to & G \\ z & \mapsto & gzg^{-1} \end{array} \mid \forall g \in G \right\}$$

Remarque: Pour tout groupe G, on a :

1. $\mathrm{Z}(G)$ est un sous-groupe de G.
2. $\mathrm{Inn}(G)$ est un sous-groupe de $\mathrm{Aut}_{Grp}(G)$.

Lemme II.0.4 *Soit G un groupe. On a :* $G/\mathrm{Z}(G) \cong \mathrm{Inn}(G)$.

Preuve (Lemme II.0.4). On introduit le morphisme :

$$\phi : \begin{array}{ccc} G & \to & \mathrm{Aut}_{Grp}(G) \\ g & \mapsto & i_g := (z \mapsto gzg^{-1}) \end{array}$$

Son image est $\mathrm{Inn}(G)$ et son noyau :

$$\begin{aligned} \mathrm{Ker}(\phi) &= \{g \in G \mid i_g = id_G\} \\ &= \{g \in G \mid \forall z \in G, gzg^{-1} = z\} \\ &= \mathrm{Z}(G) \end{aligned}$$

Ainsi par le 1^{er} théorème d'isomorphisme appliqué à ϕ on obtient que :

$$G/\mathrm{Z}(G) = G/\mathrm{Ker}(\phi) \cong Im(\phi) = \mathrm{Inn}(G)$$

□

Notation : Soit G un groupe. Soit $S \subseteq G$ une partie de l'ensemble G. On notera $\langle S \rangle$ le sous-groupe de G engendré par S, c'est-à-dire le plus petit sous-groupe de G qui contient S (ou l'intersection des sous-groupes de G contenant S).

Lemme II.0.5 *Soit G un groupe. Si $G/\mathrm{Z}(G)$ est cyclique, alors G est abélien.*

Preuve (Lemme II.0.5). Comme $G/\mathrm{Z}(G)$ est cyclique, il existe un élément $g_0 \in G$ tel que $G/\mathrm{Z}(G) = \langle \overline{g_0} \rangle$. Et donc pour tout $g \in G$, $\overline{g} = \overline{g_0}^m = \overline{g_0^m}$ pour un certain $m \in \mathbb{Z}$, donc $g \in \overline{g_0^m} = g_0^m \mathrm{Z}(G)$ et finalement il existe $z \in \mathrm{Z}(G)$ tel que $g = g_0^m z$. Ainsi si on prend $g, h \in G$, il existe $z_1, z_2 \in \mathrm{Z}(G)$ et $m, l \in \mathbb{Z}$ tel que $g = g_0^m z_1, h = g_0^l z_2$, donc on a :

$$\begin{aligned} gh &= g_0^m z_1 g_0^l z_2 \\ &= g_0^m g_0^l z_1 z_2, \text{car } z_1 \in \mathrm{Z}(G) \\ &= g_0^l g_0^m z_1 z_2 \\ &= g_0^l z_2 g_0^m z_1 \\ &= hg \end{aligned}$$

Donc G abélien. □

Preuve (Proposition II.0.2). Nous allons raisonner par l'absurde et exhiber certaines propriétés notables du groupe G dans le cas où son groupe d'automorphisme est isomorphe à $\mathbb{Z}/3\mathbb{Z}$. On peut tout d'abord faire la remarque suivante : Si G est fini et d'ordre 1 ou 2 alors son groupe d'automorphisme n'est pas isomorphe à $\mathbb{Z}/3\mathbb{Z}$ donc on peut supposer que G est soit d'ordre infini, soit d'ordre fini $n \geq 3$.

De plus, $\mathrm{Inn}(G)$ étant un sous-groupe de $\mathrm{Aut}_{Grp}(G) \cong \mathbb{Z}/3\mathbb{Z}$, on a que $\mathrm{Inn}(G)$ est isomorphe à un sous-groupe de $\mathbb{Z}/3\mathbb{Z}$, donc $\{0\}$ ou $\mathbb{Z}/3\mathbb{Z}$. Dans tous les cas $\mathrm{Inn}(G)$ est cyclique. De plus, par le Lemme II.0.4 on obtient que $\mathrm{Inn}(G) \cong G/\mathrm{Z}(G)$. Donc par le Lemme II.0.5, $G/\mathrm{Z}(G)$ étant cyclique, on a que G est abélien.

Finalement, montrons que comme G est abélien, il existe un élément d'ordre 2 dans $\mathrm{Aut}_{Grp}(G)$. Pour cela, on considère l'application :

$$\psi : \begin{array}{ccc} G & \to & G \\ x & \mapsto & x^{-1} \end{array}$$

Montrons que $\psi \in \mathrm{Aut}_{Grp}(G)$:

- ψ est un morphisme : Soient $x, y \in G$, $\psi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \psi(x)\psi(y)$ car G abélien.
- ψ est un isomorphisme car $\psi \circ \psi = id_G$, ainsi $\psi^{-1} = \psi$.

Donc $\psi \in \mathrm{Aut}_{Grp}(G)$, il nous reste à séparer les cas suivants :

- cas 1 : $\psi \neq id_G$: Dans ce cas ψ est d'ordre 2, car $\psi^1 \neq id_G$ et $\forall x \in G, \psi^2(x) = (x^{-1})^{-1} = x = id_G(x)$ donc $\psi^2 = id_G$.
- cas 2 : $\psi = id_G$: Dans ce cas, on a donc que $\forall x \in G, x^{-1} = x$ donc tous les éléments de $G \setminus \{1_G\}$ sont d'ordre 2 car $\forall x \in G \setminus \{id_G\}, x^2 = xx^{-1} = id_G$. Soit $x_0 \in G$ tel que $o(x_0) = 2$ (possible, car G infini ou d'ordre plus grand que 3 donc $G \neq \{1_G\}$), alors on a que $\langle x_0 \rangle \cong \mathbb{Z}/2\mathbb{Z}$, on définit ensuite les deux opérations suivantes :

$$\oplus : \begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & x \oplus y := xy \end{array}$$

$$\odot : \begin{array}{ccc} \langle x_0 \rangle \times G & \to & G \\ (\lambda, y) & \mapsto & \lambda \odot y := \lambda y \end{array}$$

Qui munissent ainsi G d'une structure de $\langle x_0 \rangle$-espace vectoriel, donc G est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. Et on considère une base de G : $(e_i)_{i \in I}$ pour I un ensemble.

Remarque: L'existence de bases de ces espaces et équivalente au Lemme de Zorn IV.7.6.

$(e_i)_{i \in \mathbb{I}}$ est une famille génératrice de G en tant qu'espace vectoriel et de G en tant que groupe (en rapprochant $\oplus$ et la loi de G). De plus, un morphisme de G est parfaitement déterminé si on impose l'image qu'auront les éléments de cette base. Comme $|G| \geq 3$ on a que $|I| \geq 2$ ainsi soit $i_0, i_1 \in I, i_0 \neq i_1$, il ne reste plus qu'à considérer le morphisme $\widehat{\psi}$ qui fixe tous les e_i pour $i \notin \{i_0, i_1\}$ et qui envoie $e_{i_0} \mapsto e_{i_1}$ et $e_{i_1} \mapsto e_{i_0}$ pour obtenir un élément de $\mathrm{Aut}_{Grp}(G)$ d'ordre 2.

Ainsi, on ne peut pas avoir $\mathrm{Aut}_{Grp}(G) \cong \mathbb{Z}/3\mathbb{Z}$ car dans $\mathbb{Z}/3\mathbb{Z}$ tous les éléments sont d'ordre 1 ou 3. □

On peut même étendre ces résultats pour d'autres groupes que $\mathbb{Z}/3\mathbb{Z}$.

Lemme II.0.6 *Soit H un groupe cyclique d'ordre impair. Il n'existe pas de groupe tel que son groupe d'automorphisme soit isomorphe à H.*

Preuve. La démonstration que nous avons fournie pour la Proposition II.0.2 n'utilise que le fait que le groupe H est cyclique et d'ordre impair. En effet, dans ce cas, les sous-groupes de H sont cycliques et il n'existe pas d'élément d'ordre 2 dans H (sinon 2 divise $|H|$). Donc la même preuve fournit le résultat □

Lemme II.0.7 *Il n'existe pas de groupe tel que son groupe d'automorphisme soit isomorphe à $\mathbb{Z}$.*

Preuve. $\mathbb{Z}$ est un groupe cyclique et ses sous-groupes sont cycliques : Soit K un sous-groupe de $\mathbb{Z}$ alors :

- Soit $K = \{0\}$ et alors K est cyclique.
- Soit $K \neq \{0\}$ alors il existe $x \in K \setminus \{0\}$, et $-x \in K \setminus \{0\}$ aussi. On pose $x_0 := \min(\mathbb{N} \cap (K \setminus \{0\}))$ qui est donc bien défini, et on a donc $\langle x_0 \rangle \subseteq K$. Supposons par l'absurde que $K \setminus \langle x_0 \rangle$ est non vide, soit $y \in K \setminus \langle x_0 \rangle$ et comme $\langle x_0 \rangle = x_0\mathbb{Z}$, il existe $k \in \mathbb{Z}$ tel que $kx_0 < y < (k+1)x_0$, ainsi $y - kx_0 \in K$ et $0 < y - kx_0 < x_0$, ce qui contredit la minimalité de x_0. Donc $K = \langle x_0 \rangle$ est cyclique.

De plus dans $\mathbb{Z}$ il n'y a pas d'élément d'ordre 2 en effet si $x \in \mathbb{Z}$:

- Soit $x = 0$ alors $o(x) = 1$
- Soit $x \neq 0$ et alors $\langle x \rangle = x\mathbb{Z}$ de cardinal infini.

Ainsi, on peut dérouler la démonstration de la même façon que la précédente et obtenir le même résultat pour $\mathbb{Z}$. □

III Graphes finis

III.1 Définitions et cadre

Definition III.1.1 Un *graphe* (ou *graphe orienté*) X est un couple (V, E) où :

- V est un ensemble d'éléments nommés *sommets*.
- $E \subseteq V^2$ est composé de couples représentant les connections directes entre les sommets que nous appellerons *arêtes*.

On notera les éléments de E : $[x, y]$ (ou plus rarement "(x, y)") en se souciant de l'ordre. Ainsi dans l'arête $[x, y]$, x est la base de la flèche et y est le but de la flèche (là où celle-ci pointe). Et on appellera arête *sortante* (respectivement *entrante*) de $x \in V$, une arête de la forme $[x, y]$ (respectivement $[y, x]$), pour $y \in V$.

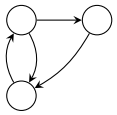


FIGURE 1 – Exemple de graphe orienté

Notation : Si on a un graphe donné X, on notera parfois $V(X)$ les sommets de X et $E(X)$ les arêtes.

Remarque: La définition donnée ci-dessus définie enfaite les graphes *simples*, c'est-à-dire ceux pour lequel il n'y a pas plusieurs fois une même arête entre deux sommets dans l'ensemble des arêtes. Dans toute la suite, nous ne considérerons donc que des graphes simples.

Par opposition aux graphes "orientés" on peut définir :

Definition III.1.2 Un graphe *non orienté* $X = (V, E)$ est un graphe (orienté, de la définition III.1.1) tel que :

$$\forall (x, y) \in V^2, [x, y] \in E \Rightarrow [y, x] \in E$$

Dans ce type de graphe, l'ordre des arêtes n'a pas d'importance, on pourra même dire que : $[x, y] = [y, x]$, ainsi on ne voit plus les arêtes comme des couples, mais plutôt comme des ensembles : $[x, y] = \{x, y\}$.

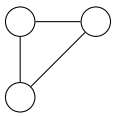


FIGURE 2 – Exemple de graphe non-orienté

Remarque: Dans le cas où il n'est pas important de le spécifier, on dénotera par "graphe" un graphe orienté ou non orienté. Par conséquent, nous spécifierons bien lorsqu'un énoncé est valable seulement pour un type de graphe.

Definition III.1.3 Soit $X = (V, E)$ un graphe. On dit que X est *sans boucle* si pour tout $x \in V$, $[x, x]$ n'est pas une arête.

Definition III.1.4 Soit $X = (V, E)$ un graphe et $\mathcal{A}$ un ensemble. On appelle *coloration* de X une application :

$$c : \begin{array}{ccc} E & \to & \mathcal{A} \\ e = [x, y] & \mapsto & c(x, y) \end{array}$$

Definition III.1.5 Soit $X = (V, E)$ un graphe. Un *sous-graphe* de X est un graphe $Y = (V_Y, E_Y)$ tel que :

$$V_Y \subseteq V, \quad E_Y \subseteq E \cap \{[x, y] \mid (x, y) \in V_Y^2\}$$

Toujours en considérant ou non l'ordre des arêtes.

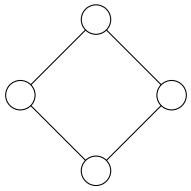
Definition III.1.6 Soit un $X = (V, E)$ un graphe non orienté et g un sommet de X on appelle *degré* de g, noté $\deg(g)$, le nombre de voisins de g, c'est-à-dire :

$$\deg(g) := |\{y \in V \mid [x, y] \in E\}|$$

Dans le cas où V est infini, on dira que c'est la cardinalité de l'ensemble $\{y \in V \mid [x, y] \in E\}$, ce qui peut être un ordinal (*cf. IV.5.3*).

Definition III.1.7 Soit $X = (V, E)$ un graphe orienté ou non et $n \geq 3$. On dit que X est un *n-cycle* si $V = \{v_1, ..., v_n\}$ et si $E = \{[v_i, v_i + 1] \mid i \in [\![1, n-1]\!]\} \cup \{[v_n, v_1]\}$.

Exemple: Le 4-cycle :



Definition III.1.8 Soit $X = (V_X, E_X), Y = (V_Y, E_Y)$ deux graphes, un *morphisme* de graphe est une application $f : V_X \to V_Y$ telle que :

$$\forall (u, v) \in V^2, ([u, v] \in E_X \Rightarrow [f(u), f(v)] \in E_Y)$$

Remarque: On peut donc définir la catégorie des graphes notée *Graph* telle que les objets sont les graphes, les morphismes sont les morphismes de graphes et la composition est la composition d'ensembles (en particulier ici l'ensemble des sommets). On peut voir que c'est une catégorie localement petite.

⚠ La catégorie des *Graph* contient les graphes orientés et non orientés donc aussi les morphismes d'un graphe orienté à un graphe non orienté, ce qui ne pose pas de problème.

De la même manière que pour une catégorie en général, on peut définir pour *Graph* les isomorphismes :

Definition III.1.9 Soit X, Y deux graphes, un *isomorphisme* de graphe de X vers Y est un morphisme $f : V(X) \to V(Y)$ de graphe, tel qu'il existe $g : V(Y) \to V(X)$ un morphisme vérifiant :

$$f \circ g = id_{V(Y)}, \quad g \circ f = id_{V(X)}.$$

S'il existe un isomorphisme de graphe de X vers Y, on dit que X et Y sont *isomorphes*. On le notera $X \cong Y$.

Definition III.1.10 Soit X un graphe orienté ou non orienté, on peut définir l'*ensemble des automorphismes* de X : $\mathrm{Aut}_{Graph}(X)$. Contenant les isomorphismes de X dans lui-même.

L'énoncé suivant reprend l'énoncé de la Propriété I.2.4 qui s'appliquait aux catégories localement petites, nous en redonnons une démonstration similaire pour se familiariser avec les notations.

Propriété III.1.11 *Soit $X = (V, E)$ un graphe orienté ou non orienté.* $\mathrm{Aut}_{Graph}(X)$ *est un groupe pour la loi de composition "$\circ$", de neutre :*

$$id : \begin{array}{ccc} V & \to & V \\ x & \mapsto & x \end{array}$$

Preuve. Soient $\alpha, \beta \in \mathrm{Aut}_{Graph}(X)$, on a que $\alpha \circ \beta$ va de V dans V et comme α et β sont des bijections, $\alpha \circ \beta$ aussi. De plus, si $[x, y] \in E$ alors $[\beta(x), \beta(y)] \in E$ et $[\alpha \circ \beta(x), \alpha \circ \beta(y)] \in E$ donc $\alpha \circ \beta$ est un morphisme de X. On peut faire le même calcul pour $(\alpha \circ \beta)^{-1}$. Donc $\circ$ est bien une loi interne sur $\mathrm{Aut}_{Graph}(X)$. Vérifions que c'est un groupe :

- Associativité : On sait que la composition est associative sur $\mathcal{F}(V, V)$ donc l'est en particulier sur $\mathrm{Aut}_{Graph}(X)$.
- Neutre : id est bien le neutre, car on a : $\alpha \circ id = \alpha = id \circ \alpha$.
- Inverse : Soit $\alpha \in \mathrm{Aut}_{Graph}(X)$, on prend α^{-1} la bijection réciproque. On sait que α^{-1} est un morphisme par définition d'isomorphisme et que $\alpha^{-1} \circ \alpha = \alpha \circ \alpha^{-1} = id_V = id$.

Ainsi $\mathrm{Aut}_{Graph}(X)$ est bien un groupe. □

Remarque: Des définitions ci-dessus, nous pouvons faire plusieurs remarques pour se familiariser avec les notions :

1. Si $X = (V, E)$ est un graphe, un élément de $\mathrm{Aut}_{Graph}(X)$ est également un élément du groupe symétrique $\mathfrak{S}(V)$.
2. On peut définir un graphe $X = (V, E)$ à l'aide de la matrice des arêtes correspondantes définie par :

$$M(X) := (m_{ij})_{(i,j)\in V^2}, \forall (i, j) \in V^2, m_{ij} = \begin{cases} 1 & \text{si } [i, j] \in E \\ 0 & \text{sinon} \end{cases}$$

On peut avoir une autre caractérisation des automorphismes. Tout d'abord on peut rappeler que si on se fixe $\sigma \in \mathfrak{S}(V)$ alors la matrice :

$$P_\sigma := (\delta_{i,\sigma(j)})_{i,j\in V^2}$$

est une matrice de permutation et $P_\sigma^{-1} = P_{\sigma^{-1}}$. On a de plus la relation :

$$\sigma \in \mathrm{Aut}_{Graph}(X) \Leftrightarrow P_\sigma M(X) = M(X) P_\sigma$$

En effet, on fait tout d'abord le calcul : Soient $(u, v) \in V^2$,

$$\begin{aligned} [P_\sigma^{-1} M(X) P_\sigma]_{u,v} &= \sum_{k\in V} [P_{\sigma^{-1}}]_{u,k} [M(X) P_\sigma]_{k,v} \\ &= \sum_{k\in V} \delta_{u,\sigma^{-1}(k)} [M(X) P_\sigma]_{k,v} \\ &= [M(X) P_\sigma]_{\sigma(u),v} \\ &= \sum_{k\in V} [M(X)]_{\sigma(u),k} [P_\sigma]_{k,v} \\ &= \sum_{k\in V} [M(X)]_{\sigma(u),k} \delta_{k,\sigma(b)} \\ &= [M(X)]_{\sigma(u),\sigma(b)} \end{aligned}$$

Donc $([M(X)]_{u,v})_{(u,v)\in V^2} \equiv ([M(X)]_{f(u),f(v)})_{(u,v)\in V^2}$ et ainsi on obtient les équivalences suivantes :

$$\begin{aligned}\sigma \in \mathrm{Aut}_{Graph}(X) &\Leftrightarrow \forall (u,v) \in V^2, ([u,v] \in E \Leftrightarrow [\sigma(u),\sigma(v)] \in E)\\ &\Leftrightarrow \forall (u,v) \in V^2, ([M(X)]_{u,v} = 1 \Leftrightarrow [M(X)]_{f(u),f(v)} = 1)\\ &\Leftrightarrow ([M(X)]_{u,v})_{(u,v)\in V^2} \equiv ([M(X)]_{f(u),f(v)})_{(u,v)\in V^2}\\ &\Leftrightarrow M(X) = P_\sigma^{-1} M(X) P_\sigma\end{aligned}$$

3. La détermination de Aut_{Graph} ne prend pas en compte la différence entre les graphes tels que pour tout sommet x, l'arête $[x,x]$ est une arête du graphe, aux graphes pour lequel aucun $[x,x]$ est une arête.
   Dans la suite, on utilisera les résultats que nous prouverons indépendamment dans les deux situations précédentes.

III.2 Quelques exemples et propriétés

III.2.1 Graphe image

Nous venons de définir la notion de sous-graphe et celle de morphisme, nous allons donc définir la notion naturelle qui suit et montrer une propriété qui sera important dans la suite.

Definition III.2.1 Soit $X = (V_X, E_X)$ un graphe, $Y = (V_Y, E_Y)$ un sous-graphe de X et α un morphisme de graphe de X vers Y. Le *graphe image* de Y par α, noté $\alpha(Y)$, est $(V_{\alpha(Y)}, E_{\alpha(Y)})$ où :

$$\begin{aligned}V_{\alpha(Y)} &= \alpha(V_Y)\\ E_{\alpha(Y)} &= \{[\alpha(a),\alpha(b)] \mid a,b \in V_Y, [a,b] \in E_Y\}\end{aligned}$$

Lemme III.2.2 *Si X un graphe, Y un sous-graphe de X et $\alpha \in \mathrm{Aut}_{Graph}(X)$. Alors, on a que Y est isomorphe à $\alpha(Y)$.*

Preuve. Soit $Y = (V_Y, E_Y)$ un sous-graphe de $X = (V_X, E_X)$ et $\alpha \in \mathrm{Aut}_{Graph}(X)$. On note $\alpha(Y) = (V_{\alpha(Y)}, E_{\alpha(Y)})$ et on considère l'application :

$$\beta : \begin{array}{ccc} V_Y & \to & V_{\alpha(Y)} \\ x & \mapsto & \alpha(x)\end{array}$$

On peut tout d'abord voir que β est une application et qu'elle est surjective, par définition de $V_{\alpha(Y)}$. L'injectivité vient du fait que α est injective et que β en est une restriction à Y. Ainsi β est bijective, il nous reste à voir que β et β^{-1} sont des morphismes de graphes :

Soient $a,b \in V_Y$ tels que $[a,b] \in E_Y$, alors $[a,b]$ est aussi une arête de X, donc $[\beta(a),\beta(b)] = [\alpha(a),\alpha(b)]$ est une arête de X et $a,b \in V_Y$, ainsi par définition de $E_{\alpha(Y)}$, $[\beta(a),\beta(b)] \in E_{\alpha(Y)}$. Donc β est un morphisme de graphe et on fait de même avec β^{-1} et α^{-1} pour obtenir que : β est un isomorphisme de graphe de Y dans $\alpha(Y)$. □

Lemme III.2.3 *Soit X, Y deux graphes non orientés, soit g un sommet de X et, soit α un isomorphisme de X vers Y. On a que* $\deg(g) = \deg(\alpha(g))$.

Preuve. Avec les notations de l'énoncé, on sait que dans X il existe $\deg(g)$ arêtes dont un des sommets est g. Comme α est un isomorphisme, on a que : pour tout h sommet de X, $[g,h]$ arête de X si et seulement si $[\alpha(g),\alpha(h)]$ arête de Y. Donc dans Y il existe également $\deg(g)$ arêtes dont un des sommets est g. Donc $\deg(g) = \deg(\alpha(g))$. □

Remarque: Des deux lemmes précédents, on peut faire de nombreuses remarques sur l'image de certains sous-graphes par un isomorphisme. Par exemple :

— Un n-cycle est envoyé sur un n-cycle.

— Une ligne de n sommets est envoyée sur une ligne de n sommets.

III.2.2 Graphes complets

On va maintenant s'intéresser à déterminer plus précisément $\mathrm{Aut}_{Graph}(X)$ dans certains cas particuliers.

Definition III.2.4 Un graphe $X = (V, E)$ est *complet* si :

$$\forall a, b \in V, a \neq b, [a,b] \in E$$

Remarque: On peut faire deux remarques sur la définition :

1. Si X est complet alors il est sans boucle et on a :

$$M(X) = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix} - Id = J - Id$$

2. On peut modifier la définition pour également considérer les arêtes "$[x,x]$", cela ne changera pas les résultats suivants dans l'ensemble.

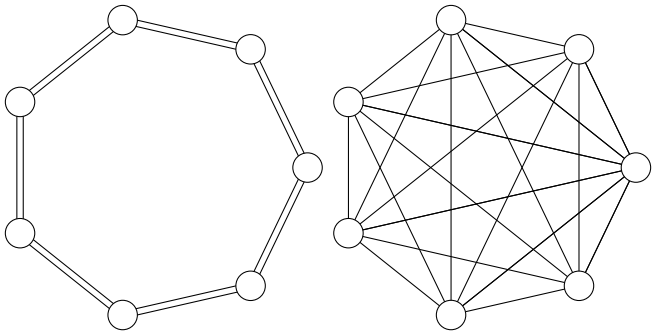
Propriété III.2.5 *Soit $X = (V, E)$ un graphe sans boucle. Si $|V| = 1$ ou $|E| > 0$ alors :*

$$X \text{ complet } \Leftrightarrow \mathrm{Aut}_{Graph}(X) \cong \mathfrak{S}(V)$$

Preuve. Supposons tout d'abord que X est complet. On a tout d'abord, en utilisant la remarque (1) précédente, que $\mathrm{Aut}_{Graph}(X)$ est isomorphe à un sous-groupe de $\mathfrak{S}(V)$. Soit $\sigma \in \mathfrak{S}(V)$, on sait par la remarque (2) précédente que σ est un élément de $\mathrm{Aut}_{Graph}(X)$ si et seulement si sa matrice de permutation P_σ commute avec $M(X) = J - Id$. Or on obtient que $P_\sigma Id = IdP_\sigma$ et $P_\sigma J = JP_\sigma$, donc on a bien $\mathrm{Aut}_{Graph}(X) \cong \mathfrak{S}(V)$.

Réciproquement, supposons que $\mathrm{Aut}_{Graph}(X) \cong \mathfrak{S}(V)$. Si $|V| = 2$ on vérifie trivialement que X est connexe. Supposons que $|V| \geq 3$. Comme $|E| > 0$ on peut se fixer $a, b \in V^2$ tel que $a \neq b$ et $[a,b] \in E$. Soient $c, d \in V^2$ tels que $c \neq d$, on considère $\sigma = (a\,c)(b\,d) \in \mathfrak{S}(V)$. Alors, on obtient que $(c,d) = (\sigma(a), \sigma(b))$ est une arête de X car $\sigma \in \mathrm{Aut}_{Graph}(X)$. Donc X est complet. □

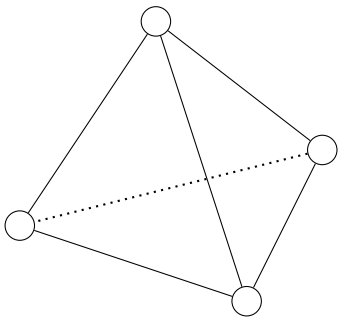
Notation : Pour noter un graphe complet à n sommets sans encombrer le dessin, on utilisera un graphe cycle avec des arêtes doublées. Par exemple :



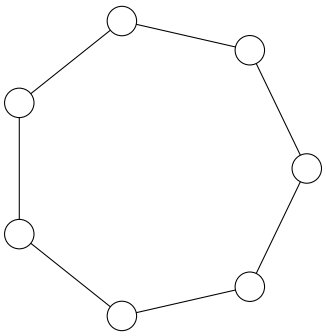
désignent le même graphe.

Exemple: D'autres exemples :

— Le groupe d'automorphisme du tétraèdre est $\mathfrak{S}_4$ car le graphe du tétraèdre est complet.



— Le groupe d'automorphisme d'un n-cycle est le groupe diédral D_{2n}.



En effet, on sait tout d'abord que D_{2n} est le groupe des isométries du n-gone régulier. On peut vérifier que si on note 1,...,n les éléments de $V(X)$ et les sommets du n-gone régulier, alors un automorphisme de graphe est une isométrie du n-gone ce qui se voit facilement en utilisant le fait qu'un graphe ligne s'envoie sur un graphe ligne. De plus, si on prend une isométrie du n-gone régulier, alors en faisant correspondre les sommets successifs du n-gone régulier avec les sommets successifs du graphe cycle on obtient un automorphisme de graphe.

III.2.3 Graphes connexes

On supposera dans la suite que X est un graphe non orienté sans boucles. Une remarque importante dans l'étude de $\mathrm{Aut}_{Graph}(X)$ est le fait qu'on peut se restreindre à l'étude des graphes connexes :

Definition III.2.6 Soit $X = (V, E)$ un graphe, soient $a, b \in V$ on dirait que a et b sont *connectés* s'il existe une suite $(u_n)_{n\in[\![0,N]\!]} \in V^N$ telle que $u_1 = a$, $u_N = b$ et pour tout $n \in [\![1, ..., N-1]\!]$ on a $[u_n, u_{n+1}] \in E$. On dira de plus que X est *connexe* si : $\forall a, b \in V, a \neq b$, a et b sont connectés.

Dans le cas d'un graphe non forcément connexe, on peut également définir :

Definition III.2.7 Soit $X = (V, E)$ un graphe, soit $x \in V$, on appelle *composante connexe de* x, le plus grand sous-graphe $Y = (V_Y, E_Y)$ de X tel que Y soit connexe et $x \in V_Y$. On dira plus généralement que Y est une *composante connexe* de X.

Nous allons définir maintenant la notion de "graphe somme" pour aboutir sur la décomposition en graphes connexes, qui nous intéressait au départ.

Definition III.2.8 Soit B un ensemble et $\{X_b = (V_{X_b}, E_{X_b}) \mid b \in B\}$ un ensemble de graphes. On définit le graphe *somme*, noté $\sum_{b\in B} X_b$, de la façon suivante :

$$V(\sum_{b\in B} X_b) := \bigcup_{b\in B}(\{b\} \times V_{X_b}),$$
$$E(\sum_{b\in B} X_b) := \{[(b, x), (b, y)] \mid b \in B, [x, y] \in E_{X_b}\}$$

Remarque: Il est donc possible de décomposer un graphe X comme somme de ses composantes connexes. En effet, si on note $\{Y_j, j \in J\}$ les composantes connexes de X. On peut voir que $X \cong \sum_{j\in J} Y_j$, en identifiant simplement les arêtes $[(j, x), (j, y)]$ avec les arêtes $[x, y]$ dans X qui servaient à les définir par l'isomorphisme :

$$\begin{array}{ccc} V_X & \to & V(\sum_{j\in J} Y_j) \\ x & \mapsto & (j, x) \text{ si } x \in Y_j \end{array}$$

Proposition III.2.9 *Soit X un graphe, on va noter $(X_{i,j})_{i\in I, j\in J_i}$ les différentes composantes connexes de X, tel que pour tout $i \in I$, $(X_{i,j})_{j\in J_i}$ est une famille de graphes isomorphes deux à deux et tel que pour tous i', j' si $i' \neq i$, $X_{i',j'}$ n'est isomorphe à aucun des $(X_{i,j})_{j\in J_i}$. On définit $X_i = \sum_{j\in J_i} X_{i,j}$. On a déjà vu $X \cong \sum_{i\in I} X_i$ et on a :*

$$\begin{aligned} \mathrm{Aut}_{Graph}(X) &\cong \mathrm{Aut}_{Graph}(X_1) \times ... \times \mathrm{Aut}_{Graph}(X_i) \times ... \\ &\cong \bigtimes_{i\in I} \mathrm{Aut}_{Graph}(X_i) \end{aligned}$$

Preuve. On reprend les notations de l'énoncé en posant :

$$X = (V, E) \text{ et } (X_i)_{i\in I} = ((V_i, E_i))_{i\in I}$$

Nous allons exhiber l'isomorphisme entre ces groupes. Soit $\alpha \in \mathrm{Aut}_{Graph}(X)$, on sait par le Lemme III.2.2, que pour tous $i \in I, j \in J_i$, $\alpha_{|_{X_{i,j}}}$ est un isomorphisme de $X_{i,j}$ dans $\alpha(X_{i,j})$. Ainsi $\alpha(X_{i,j}) = X_{i,j'}$ pour un $j' \in J_i$ par définition des $(X_{i,j})_{i\in I, j\in J_i}$. On peut faire pareil pour montrer que $\alpha_{|_{X_i}}$ est un isomorphisme de X_i dans X_i, en effet, c'est une bijection comme restriction d'une bijection sur un sous-ensemble

stable (ici X_i) et c'est un morphisme en observant que les arêtes de X_i sont envoyées sur les arêtes de X_i et qu'il n'y a pas d'arêtes d'un sommet de X_i vers un sommet de $X_{i'}$ par connexité. Ainsi $\alpha_{|X_i} \in \mathrm{Aut}_{Graph}(X_i)$. On pose :

$$\chi : \begin{array}{ccc} \mathrm{Aut}_{Graph}(X) & \to & \bigtimes_{i\in I} \mathrm{Aut}_{Graph}(X_i) \\ \alpha & \mapsto & (\alpha_{|X_1}, ..., \alpha_{|X_i}, ...) \end{array}$$

Montrons que χ est un isomorphisme de groupe.

— Morphisme : Soit $\alpha_1, \alpha_2 \in \mathrm{Aut}_{Graph}(X)$, on a pour tout $i \in I$, $\alpha_{1|X_i} \circ \alpha_{2|X_i} = (\alpha_1 \circ \alpha_2)_{|X_i}$, ainsi :

$$\begin{aligned} \chi(\alpha_1 \circ \alpha_2) &= ((\alpha_1 \circ \alpha_2)_{|X_1}, ..., (\alpha_1 \circ \alpha_2)_{|X_i}, ...) \\ &= (\alpha_{1|X_1} \circ \alpha_{2|X_1}, ..., \alpha_{1|X_i} \circ \alpha_{2|X_i}, ...) \\ &= (\alpha_{1|X_1}, ..., \alpha_{1|X_i}, ...) \circledcirc (\alpha_{2|X_1}, ..., \alpha_{2|X_i}, ...) \\ &= \chi(\alpha_1) \circledcirc \chi(\alpha_2), \end{aligned}$$

où $\circledcirc$ est la loi sur $\bigtimes_{i\in I} \mathrm{Aut}_{Graph}(X_i)$ définie comme la composition composante par composante. Donc χ morphisme.

— Injectivité : Soit $\alpha_1, \alpha_2 \in \mathrm{Aut}_{Graph}(X)$ tels que $\chi(\alpha_1) = \chi(\alpha_2)$, alors :

$$(\alpha_{1|X_1}, ..., \alpha_{1|X_i}, ...) = (\alpha_{2|X_1}, ..., \alpha_{2|X_i}, ...).$$

Ainsi pour tous $i \in I, x \in V_i$,

$$\begin{aligned} \alpha_1(x) &= \alpha_{1|X_i}(x) \\ &= \alpha_{2|X_i}(x) \\ &= \alpha_2(x) \end{aligned}$$

Donc $\alpha_1 = \alpha_2$, donc χ injective.

— Surjectivité : Soient $(\beta_1, ..., \beta_i, ...) \in \bigtimes_{i\in I} \mathrm{Aut}_{Graph}(X_i)$ alors on définit :

$$\alpha : \begin{array}{ccc} V_X & \to & V_X \\ x & \mapsto & \beta_i(x) \text{ où } x \in V_i \end{array}$$

On voit directement que α est bien défini et qu'il définit un morphisme bijectif, car les β_i sont des automorphismes. Donc χ surjective.

Ainsi $\mathrm{Aut}_{Graph}(X) \cong \bigtimes_{i\in I} \mathrm{Aut}_{Graph}(X_i)$. □

III.3 Graphe de Cayley

Nous allons donc maintenant introduire le Graphe de Cayley qui est un graphe qui encode toute la structure d'un groupe, en particulier nous allons voir que les automorphismes de ces graphes redonne le groupe de départ.

Construction : Soit G un groupe et 1_G son neutre. On prend alors le graphe ordonné complet, avec boucle, dont les sommets sont les éléments de G. Ainsi on a $X = (G, E)$ et pour tout $(u, v) \in G^2, [u, v] \in E$.

On définit une coloration sur ce graphe par l'application :

$$c : \begin{array}{ccc} E & \to & G \\ e = [g,h] & \mapsto & g^{-1}h \end{array}$$

Et on notera dans la suite $c_{g,h} := c([g,h])$. Ainsi, on répartit les arêtes en N classes/couleurs différentes. On peut remarquer également qu'à chaque sommet x et à chaque couleur c il existe une arête entrante et une arête sortante de x de couleur c. En effet, si g est un sommet et $c = h$ une couleur, alors comme $h = g^{-1}gh$ on obtient que l'arête $[g, gh]$ est de couleur h. Ainsi on a une arête de chaque couleur sortant de g, en répétant l'argument pour tout sommet et pour les arêtes sortantes et rentrantes, on a ce qu'on veut.

Notation : On notera $\mathcal{C}(G)$ le graphe X de la construction précédente, nommé le *graphe de Cayley* de G.

Exemple: Pour le groupe $G = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$, on a :

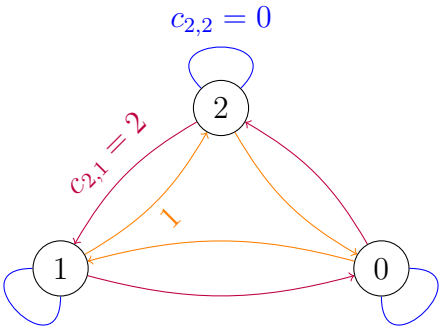


FIGURE 3 – Graphe de Cayley de $\mathbb{Z}/3\mathbb{Z}$

Propriété III.3.1 *Soit G un groupe d'ordre $N \geq 1$ fini, $\mathcal{C}(G)$ possède N^2 arêtes.*

Preuve. On note a_N le nombre d'arêtes dans $\mathcal{C}(G)$. Raisonnons par récurrence sur $N \geq 1$, on veut montrer la propriété :

$$(\mathcal{P}_N) \quad a_N = N^2$$

— Initialisation : Pour $N = 1$, $a_N = 1 = 1^2$.

— Récurrence : Soit $N \geq 1$. Supposons avoir montré $(\mathcal{P}_{N-1})$. Le graphe $\mathcal{C}(G)$ est le graphe $\mathcal{C}(G \setminus \{1_G\})$ auquel on a ajouté le sommet 1_G, l'arête $[1_G, 1_G]$ et pour chaque $x \in G \setminus \{1_G\}$ les deux arêtes : $[x, 1_G]$ et $[1_G, x]$. Donc, on a la relation :

$$\begin{aligned} a_N &= a_{N-1} + 1 + 2(N-1) \\ &= (N-1)^2 - 1 + 2N, \text{ par } (\mathcal{P}_{N-1}) \\ &= N^2 \end{aligned}$$

On conclut par récurrence. □

Remarque: Sur cette construction, on peut faire plusieurs remarques :

— Soient $g_0, ..., g_n$ des éléments de G. On a la relation suivante :

$$g_n = g_0 c_{g_0,g_1} c_{g_1,g_2} c_{g_2,g_3} ... c_{g_{n-1},g_n}.$$

— Soit $x \in G$. On sait que de tous les sommets de $\mathcal{C}(G)$ il n'y a qu'une arête sortante et une entrante de couleur x. On a de plus que s'il existe $n \in \mathbb{N}$ tel que, en partant d'un sommet g de $\mathcal{C}(G)$ et en suivant n-fois l'arête sortante de couleur x, on retombe sur g alors x est d'ordre fini dans G divisant n.

On peut faire une autre construction que celle du graphe de Cayley que nous avons décrite ci-dessus. En effet, à partir d'un groupe G et d'une famille $\mathcal{S}$ d'éléments de G qui est génératrice. On peut définir le graphe de Cayley, mais où on a gardé seulement les arêtes dont la couleur est dans $\mathcal{S}$.

Cette construction est aussi intéressante que celle du graphe de Cayley $\mathcal{C}(G)$ car elle contient toutes les informations nécessaires à la description du groupe.

Notation : On notera ce graphe $\mathcal{C}_{\mathcal{S}}(G)$.

Exemple: Pour le groupe $\mathbb{Z}/3\mathbb{Z} = \langle 1 \rangle$, on a :

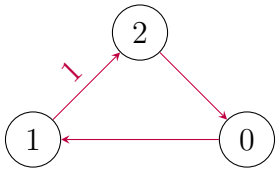


FIGURE 4 – Graphe de Cayley des générateurs de $\mathbb{Z}/3\mathbb{Z}$

III.4 Automorphisme préservant la couleur

Dans cette section, on va s'intéresser aux automorphismes du graphe de Cayley préservant la coloration.

Definition III.4.1 (Préservation de la couleur) Soient E un ensemble d'arêtes et $\mathcal{A}$ un ensemble. Soient $X = (V_X, E_X), Y = (V_Y, E_Y)$ deux graphes tels que $E_X, E_Y \subseteq E$. Soit f un morphisme de graphe de X sur Y et soient $c_X : E_X \to \mathcal{A}$ et $c_Y : E_Y \to \mathcal{A}$ deux colorations de, respectivement, X et Y. On dit que f *préserve la couleur* si une arête et son image ont la même couleur par f. Plus précisément :

$$\forall e = [a, b] \in E_X, c_X([a, b]) = c_Y([f(a), f(b)]) \in \mathcal{A}.$$

Remarque: Fixons un ensemble $\mathcal{A}$ quelconque. On peut restreindre la catégorie *Graph* sur ces morphismes et ces objets, pour considérer les graphes munis d'une coloration à valeur dans $\mathcal{A}$ et les morphismes de graphes préservant la couleur. On notera cette catégorie $Couleur_{\mathcal{A}}$ et donc le graphe de Cayley muni de sa coloration construite dans la section précédente est un élément de la catégorie.

Definition III.4.2 (Automorphismes et couleurs) Soit G un groupe.

— Les *automorphismes du graphe de Cayley préservant la couleur* sont définis comme les automorphismes de graphe de $\mathcal{C}(G) = (G, E)$ qui préservent la coloration

$$c : \begin{array}{ccc} E & \to & G \\ e = [g, h] & \mapsto & g^{-1}h. \end{array}$$

Plus précisément, un automorphisme α préserve la coloration si :

$$\forall e = [x, y] \in E, c_{x,y} = c_{\alpha(x),\alpha(y)} \text{ i.e. } x^{-1}y = \alpha(x)^{-1}\alpha(y).$$

— On notera l'ensemble des automorphismes (qui est un groupe par I.2.4) du graphe de Cayley préservant la couleur : $\mathrm{Aut}_{Couleur}(\mathcal{C}(G))$.

Remarque: Pour un groupe G donné, $\mathrm{Aut}_{Couleur}(\mathcal{C}(G))$ est donc le groupe contenant les automorphismes de la catégorie $Couleur_G$.

Il nous manque simplement la définition des morphismes de multiplication à gauche pour ensuite regarder notre premier résultat de réalisabilité sur les graphes.

Definition III.4.3 Soit G un groupe. Pour tout, $x \in G$ on définit :

$$f_x : \begin{array}{ccc} G & \to & G \\ g & \mapsto & xg \end{array},$$

l'application de *multiplication à gauche* par x.

Notation : On notera $\mathrm{Gau}(G) = \{f_x \mid x \in G\}$, l'ensemble des applications de multiplications à gauche.

Propriété III.4.4 *Soit G un groupe.* $\mathrm{Gau}(G)$ *muni de la composition est un groupe de neutre $id_G = f_{1_G}$.*

Preuve. Soient $g, h \in G$. On a $f_g \circ f_h = f_{gh}$, ainsi $\circ$ est une loi de composition interne sur $\mathrm{Gau}(G)$. De plus on a $f_g \circ f_{1_G} = f_{1_G} \circ f_g = f_g$ et $f_g^{-1} = f_{g^{-1}}$, grâce aux propriétés de groupe de G. □

Remarque: Nous verrons même que $\mathrm{Gau}(G)$ est isomorphe à G dans la Proposition III.4.6

Théorème III.4.5 *Tous les automorphismes du graphe de Cayley qui préservent la coloration des arêtes sont obtenus par multiplication à gauche des éléments du groupe.*

Preuve. Il nous faut donc montrer que :

$$\{\alpha \in \mathrm{Aut}_{Graph}(\mathcal{C}(G)), \alpha \text{ préserve la coloration}\} = \left\{ f_x : \begin{array}{ccc} G & \to & G \\ g & \mapsto & xg \end{array}, \forall x \in G \right\},$$

ou encore :

$$\mathrm{Aut}_{Couleur}(\mathcal{C}(G)) = \mathrm{Gau}(G)$$

Procédons par double inclusion,

$\supseteq$) Soit $x \in G$, comme $\mathcal{C}(G)$ est un graphe complet, on a que f_x est un morphisme de graphe, car il est défini de l'ensemble des sommets dans lui-même et les relations sur les arêtes sont toutes trivialement vérifiées. De plus f_x est injectif, car on a : $\forall g, h \in G, xg = xh \Rightarrow g = h$, et surjectif car : $\forall g \in G, g = f_x(x^{-1}g)$. De plus f_x préserve la couleur, car si on prend $g, h \in G$ alors $[g, h]$ est de couleur $c_{g,h}$ et $[f_x(g), f_x(h)] = [xg, xh]$ est de couleur $(xg)^{-1}xh = g^{-1}x^{-1}xh = c_{g,h}$. Ainsi, on a l'inclusion voulue.

$\subseteq$) Soit $\alpha \in \mathrm{Aut}_{Graph}(\mathcal{C}(G))$ préservant la couleur. Tout d'abord, on peut faire la remarque que s'il existe $g \in G$ fixé par α alors $\alpha = id$. En effet, soit $h \in G$ alors on sait que $[g, h]$ et $[\alpha(g), \alpha(h)]$ sont de même couleur, ainsi on obtient que :

$$g^{-1}h = (\alpha(g))^{-1}\alpha(h) = g^{-1}\alpha(h)$$

et donc on a $\forall h \in G, \alpha(h) = h$, c'est-à-dire $\alpha = id$. Supposons maintenant que $\alpha \neq id$ et donc que α déplace tous les sommets. Soit $g \in G \setminus 1_G$ montrons que si on a, $\alpha : 1_G \mapsto g$ alors α est complètement déterminé. En effet, supposons de plus que $\alpha : 1_G \mapsto g$. Soit $h \in G$, comme α préserve la coloration, on a que $(1_G, h)$ et $(\alpha(1_G), \alpha(h))$ sont de même couleur, ainsi on a comme précédemment $1_G^{-1}h = (\alpha(1_G))^{-1}\alpha(h) = g^{-1}\alpha(h)$, donc finalement $\forall h \in G, \alpha(h) = g1_G^{-1}h$. Donc, on a montré que α est parfaitement déterminé si on fixe simplement l'image de 1_G et de plus que α ainsi déterminé est de la forme "f_x". Ainsi, on a l'autre inclusion. □

Remarque: On rappelle que le théorème reste inchangé même si on ne considère par l'arête $[g, g]$ pour chaque élément $g \in G$, car son image est directement déterminée par l'image d'un élément et sa couleur est celle de 1_G.

Le théorème nous dit que :

Proposition III.4.6 *Soit G un groupe,* $\mathrm{Gau}(G)) \cong G$.

Preuve. En effet, l'application, $\Phi : \begin{array}{ccc} G & \to & \mathrm{Gau}(G) \\ g & \mapsto & f_g \end{array}$ vérifie :

- — Morphisme : Soient $g, h \in G$, $\Phi(gh) = f_{gh} = f_g \circ f_h = \Phi(g) \circ \Phi(h)$. Donc Φ est un morphisme de groupe.
- — Injectif : Soit $g \in G$ tel que $\Phi(g) = id_G$. On a $f_g = id = f_{1_G}$ donc $f_g(1_G) = g = f_{1_G}(1_G)$ ainsi $g = 1_G$. On a donc que $\mathrm{Ker}(\Phi) = \emptyset$. Donc Φ est injectif.
- — Surjectif : Soit $\varphi \in \mathrm{Gau}(G)$, alors il existe $g \in G$ tel que $\varphi = f_g$ donc $\Phi(g) = \varphi$. Donc Φ est surjective.

Ainsi Φ est un isomorphisme de groupe et on a que $\mathrm{Gau}(G) \cong G$. □

Finalement, nous venons de montrer avec les énoncés III.4.5 et III.4.6 que pour tout groupe G, $\boxed{\mathrm{Aut}_{Couleur}(\mathcal{C}(G)) \cong G}$.

Avec un travail similaire à celui réalisé précédemment, il est possible de préciser un peu cela et de montrer la Proposition suivante :

Proposition III.4.7 *Si on a G un groupe et $\mathcal{S}$ une partie génératrice. Alors :*

$$\mathrm{Aut}_{Couleur}(\mathcal{C}(G)) \cong \mathrm{Aut}_{Couleur}(\mathcal{C}_{\mathcal{S}}(G)) \cong G$$

III.5 Extension au cas non orienté

C'est dans cette section que nous répondrons à la question posée en montrant le théorème suivant :

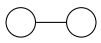
Théorème III.5.1 (Frucht) *Soit G un groupe fini. Il existe un graphe X, non orienté, fini, tel que son groupe d'automorphisme est isomorphe à G.*

Preuve (Théorème). On notera dans toute la suite $N = |G|$ et on se fixera une façon de numéroter les éléments du groupe : $G = \{g_i \mid i \in [\![1, N]\!]\}$. Séparons-nous de cas triviaux :

— Cas $N = 1$: On a que $G \cong \mathfrak{S}_1$ et on prend le graphe X suivant :

On a facilement que $\mathrm{Aut}_{Graph}(G) = G$ car X est complet et a 1 sommet.

— Cas $N = 2$: On a que $G \cong \mathfrak{S}_2$ et on prend le graphe X suivant :



On se place maintenant dans le cas $N \geq 3$, soit $i \in [\![1, N]\!]$, on définit H_i comme étant un graphe non-orienté composé de 4 sommets alignés, numérotés de 1 à 4, avec une ligne de $2i$ sommets connecté au sommet 2 et une ligne de $2i + 1$ sur le sommet 3.

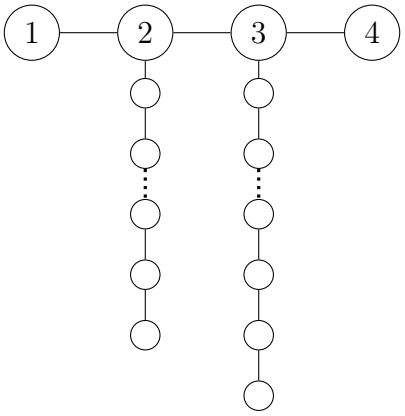


FIGURE 5 – Exemple de H_i

Nous avons introduit les $(H_k)_k$ de cette manière de façon un peu arbitraire, on entend par cela que nous utilisons des $(H_k)_k$ seulement plusieurs propriétés :

— Soit $k \in [\![1, N]\!]$, H_k est connexe.

— Soient $i, j \in [\![1, N]\!], i \neq j$, H_i et H_j ne sont pas isomorphes.

— Soit $k \in [\![1, N]\!]$, $\mathrm{Aut}_{Graph}(H_k) \cong \{id\}$. En effet, soit $\alpha \in \mathrm{Aut}_{Graph}(H_k)$, les sommets "2" et "3" de H_k sont les seuls de degré 3. Le sous-graphe A composé du sommet "2" et de la ligne de $2k$ sommets qui lui est connecté (avec un sommet de degré 1 à l'extrémité), est envoyé sur un sous-graphe du même type, donc soit lui-même, soit le sous-graphe B composé de "3" et une ligne de $2k$ sommets, mais dans ce cas le $2k+1$-ème sommet n'est pas dans B et n'y est pas connecté, car l'extrémité de A (et donc de B) est de degré 1. Ce qui est absurde. Donc, on a que "2" et "3" sont envoyés sur eux-mêmes et tous les autres sommets aussi. Ainsi $\alpha = id$.

Grâce à la construction des $(H_k)_k$, à chaque couleur, $g_i \in G$ on associe un graphe avec un nombre différent de sommets. On construit ensuite le graphe X, défini comme le graphe de Cayley, $\mathcal{C}(G)$ mais où pour tous $i \neq j$ on a remplacé l'arête $[g_i, g_j]$ de couleur $c_{g_i,g_j} = g_k$ par une copie du graphe H_k, en faisant correspondre le sommet g_i avec 1 et le sommet g_j avec 4, on a également supprimé simplement l'arête $[g_i, g_i]$. Ainsi X est non orienté et connexe, de plus seules les arêtes qui étaient de même couleur correspondent aux mêmes sous-graphes.

Soit $\alpha \in \mathrm{Aut}_{Graph}(X)$, commençons par faire deux remarques, qui nous serviront plus tard :

— Soit $g_i \in G$ alors $\alpha(g_i) \in G$. En effet, g_i est d'ordre $2N \geq 6$ dans X donc $\alpha(g_i)$ aussi par le lemme sur les degrés. Or seuls les sommets qui sont des éléments de G sont de degré $2N$ car les autres ont au maximum 2 voisins, ainsi $\alpha(g_i)$ est envoyé sur un élément de G.

— Considérons-le sous graphe $\tilde{X}$ de X composé des sommets de X qui ne sont pas des éléments de G. Ce graphe a $N^2 - N$ composantes connexes correspondants à tous les graphes copies des H_k (sans leurs sommets "1" et "4" que l'on fait correspondent à des éléments de G) que l'on avait ajouté dans la construction de X. De plus, avec la remarque précédente, on a que α envoie les éléments de G sur les éléments de G, or étant un isomorphisme, il envoie les éléments qui ne sont pas dans G vers d'autres que ne sont pas dedans. Ainsi, en restriction au sous-graphe $\tilde{X}$, α est un automorphisme. Donc, il envoie une composante connexe de $\tilde{X}$ sur une autre composante connexe. Soient $g_i, g_j \in G$, si on considère un sous-graphe $H_k^{(1)}$ (copie de H_k) de couleur g_k qui les relie :

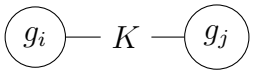
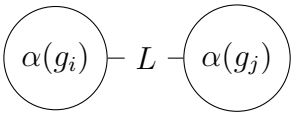


FIGURE 6 – $H_k^{(1)}$

K étant une composante connexe de $\tilde{X}$ il est envoyé sur une autre composante connexe L et ainsi $H_k^{(1)}$ est envoyé sur le graphe composé de $\alpha(g_1)$, L et $\alpha(g_2)$.



Ce graphe ne peut être qu'un H_l par définition de X, on le notera $H_l^{(2)}$. On sait de plus que $H_k^{(2)}$ est isomorphe à $H_l^{(2)}$, ainsi $k = l$. En résumé, on a que la copie de H_k, $H_k^{(1)}$ dans laquelle se trouve g_i et g_j est envoyé par α sur une autre copie, $H_k^{(2)}$ dans laquelle se trouve $\alpha(g_i)$ et $\alpha(g_j)$. Mais on a que $\mathrm{Aut}_{Graph}(H_k) \cong \{id\}$, ainsi il n'y a qu'une façon d'envoyer une copie de H_k sur une autre copie, c'est en considérant "l'identité" sur ces copies. Plus précisément, les sommets correspondants à ceux numérotés 1 à 4 dans H_k sont envoyés sur les autres sommets correspondants dans l'autre copie et les lignes de même.

Finalement, il nous reste à faire correspondre $\mathrm{Aut}_{Graph}(X)$ et $\mathrm{Aut}_{Couleur}(\mathcal{C}(G))$. Pour cela on considère l'application :

$$\chi : \begin{array}{ccc} \mathrm{Aut}_{Graph}(X) & \to & \mathrm{Aut}_{Couleur}(\mathcal{C}(G)) \\ \alpha & \mapsto & \alpha_{|_{\mathcal{C}(G)}} \end{array}$$

où $\alpha_{|_{\mathcal{C}(G)}}$ est la restriction de α aux sommets de X qui étaient des sommets de $\mathcal{C}(G)$ avant la construction.

Montrons que cette application est bien définie, qu'elle définit un morphisme de groupe et que ce morphisme est bijectif :

1. Bien définie : Soit $\alpha \in \mathrm{Aut}_{Graph}(X)$, il est aisé de voir que $\alpha_{|_{\mathcal{C}(G)}}$ défini une bijection grâce à la première remarque précédente (les sommets de $\mathcal{C}(G)$ étant les éléments de G ils sont envoyés sur des éléments de G et comme α est une bijection $\alpha_{|_{\mathcal{C}(G)}}$ aussi). Il nous reste à voir que $\alpha_{|_{\mathcal{C}(G)}}$ est bien un morphisme de graphe de $\mathcal{C}(G)$ dans $\mathcal{C}(G)$, ce qui est aussi immédiat, car dans $\mathcal{C}(G)$ tous les 2-tuples sont des arêtes. On en déduit la même chose pour $\alpha^{-1}_{|_{\mathcal{C}(G)}}$ et on a que $\alpha_{|_{\mathcal{C}(G)}}$ est bien un automorphisme donc χ bien définie.
2. Morphisme : Soient $(\alpha, \beta) \in \mathrm{Aut}_{Graph}(X)^2$, on doit montrer que :

$$\chi(\alpha \circ \beta) = \chi(\alpha) \circ \chi(\beta)$$

   Ceci est une égalité d'application de $\mathrm{Aut}_{Couleur}(\mathcal{C}(G))$, ainsi soit h un sommet de $\mathcal{C}(G)$, on a que :

$$\begin{aligned}\chi(\alpha \circ \beta)(h) &= (\alpha \circ \beta)_{|_{\mathcal{C}(G)}}(h)\\ &= (\alpha \circ \beta)(h)\\ &= \alpha \circ \beta(h)\\ &= \alpha_{|_{\mathcal{C}(G)}} \circ \beta_{|_{\mathcal{C}(G)}}(h)\\ &= \chi(\alpha) \circ \chi(\beta)(h)\end{aligned}$$

   Donc χ est un morphisme.
3. Injectivité : Soient $\alpha \in \mathrm{Aut}_{Graph}(X)$ tels que $\chi(\alpha) = id_{\mathrm{Aut}_{Couleur}(\mathcal{C}(G))}$. Ainsi α fixe tous les sommets dans G. Soit h un sommet de $X \setminus G$ alors h est un sommet d'une copie d'un H_k qui correspond à une arête de couleur $g_k = c_{g_i,g_j}$ telle que g_i et g_j sont les extrémités de cette copie. Par les remarques, on a que g_i et g_j sont fixés par α et que la copie de H_k est envoyée sur une autre copie de H_k connecté à $\alpha(g_i) = g_i$ et à $\alpha(g_j) = g_j$, par le morphisme représentant "l'identité" (mais ici pour les copies) du groupe $\mathrm{Aut}_{Graph}(H_k)$, or dans $\mathcal{C}(G)$ il n'y a qu'une arête connectée à g_i et g_j de couleur g_k, donc on en déduit que la copie de H_k dans laquelle h se trouve est envoyé sur elle-même et donc que le sommet h est envoyée sur lui-même. Finalement α fixe tous les éléments de X donc χ est injective, car c'est un morphisme de groupes.
4. Surjective : Soit $\beta \in \mathrm{Aut}_{Couleur}(\mathcal{C}(G))$. On prend $\alpha \in \mathrm{Aut}_{Graph}(X)$ tel que pour $h \in V(X)$,
   - si $h \in \mathcal{C}(G)$, $\alpha(h) = \beta(h)$
   - sinon on sélectionne le sous graphe contenant un g_i, un g_j et qui est une copie de H_k tel que h est dans cette copie et on définit l'image de h comme l'unique élément correspondant dans l'autre copie de H_k qui contient $\alpha(g_i)$ et $\alpha(g_j)$. On peut vérifier que α ainsi défini est bien un automorphisme de X dans X.

   On a donc défini un élément de $\alpha \in \mathrm{Aut}_{Graph}(X)$ tel que $\chi(\alpha) = \beta$ donc χ est surjective.

Donc χ est un isomorphisme de groupe, ainsi :

$$\mathrm{Aut}_{Graph}(X) \cong \mathrm{Aut}_{Couleur}(\mathcal{C}(G)) \cong G$$

On a donc trouvé un graphe X réalisant G, ce qui termine la preuve. □

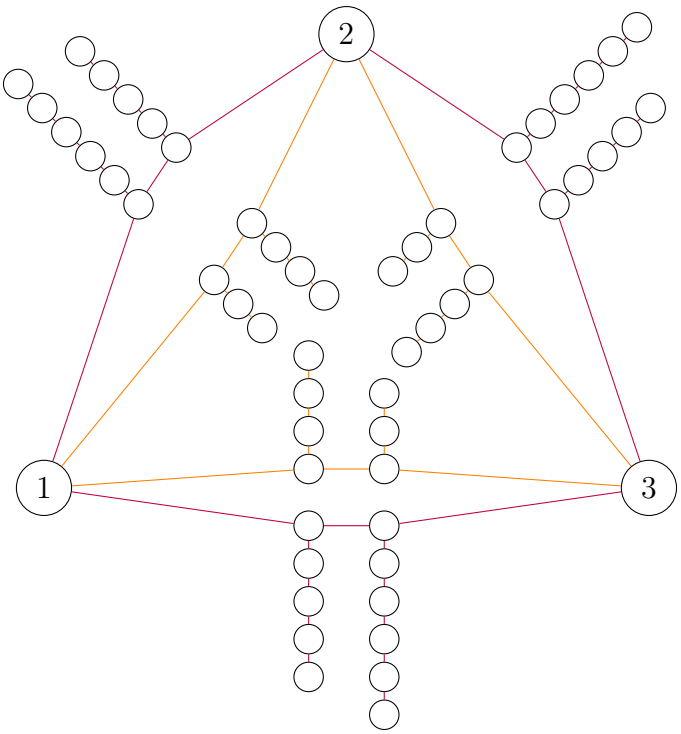


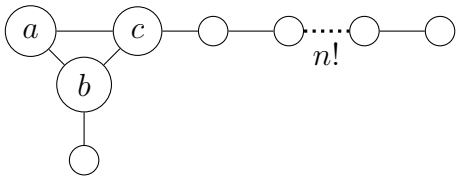
FIGURE 7 – Graphe du théorème pour le groupe $\mathbb{Z}/3\mathbb{Z}$

Étendons un tout petit peu ce théorème :

Corrolaire III.5.2 *Soit G un groupe fini. Il existe une infinité de graphes X, non orientés, finis, tel que leur groupe d'automorphisme est isomorphe à G.*

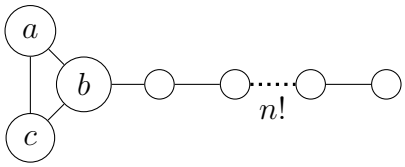
Preuve. On notera comme précédemment $N = |G|$. Séparons-nous de cas triviaux :

— Cas $N = 1$: On a que $G \cong \{1_G\}$. Soit $n \in \mathbb{N}$, on construit le graphe X_n contenant un cycle de taille 3 avec un des sommets du cycle aussi connecté à un autre sommet et un autre sommet du cycle connecté à une ligne de $2 + n!$ sommets.



Soit $\alpha \in \mathrm{Aut}_{Graph}(X_n)$ alors le 3-cycle est préservé par α, de plus on peut voir que c est envoyé sur c car le sous-graphe contenant c et la ligne connectée à c ne peut être envoyée que sur elle-même. On en déduit pareil pour b et a et ainsi $\alpha = id_{X_n}$. Donc $\forall n \in \mathbb{N}, \mathrm{Aut}_{Graph}(X_n) \cong G$.

— Cas $N = 2$: On a que $G \cong \mathbb{Z}/2\mathbb{Z}$. Soit $n \in \mathbb{N}$ on construit X_n de la façon suivante :



Et on peut voir que si $\alpha \in \mathrm{Aut}_{Graph}(X_n)$ alors α est, soit id_X soit est la permutation qui échange a et c. Donc $\forall n \in \mathbb{N}, \mathrm{Aut}_{Graph}(X_n) \cong G$.

On se place maintenant dans le cas $N \geq 3$. De manière générale, il suffit de dérouler la même démonstration que pour le Théorème III.5.1 avec d'autres constructions de "H_k". On a fait la remarque qu'il faut simplement s'assurer que l'on construit N graphes connexes non isomorphes deux à deux et tel que le groupe d'automorphisme est, $\{id\}$ car ainsi les remarques faites au début de la démonstration du Théorème seront encore valables pour les nouveaux H_k et tout se passera bien. Pour définir de nouveau "H_k", on peut raisonner de la manière suivante : Soit $n \in \mathbb{N}$, pour tout $k \in [\![1, N]\!]$, on pose $\widehat{H}_k^{(n)} := H_{n.k}$, où "$(H_k)_k$" désigne la construction que l'on avait faite dans la preuve du Théorème et "$(\widehat{H}_k^{(n)})_k$" la nouvelle construction, et ainsi la démonstration marche de la même manière avec les $(H_k)_k$ ou les $(\widehat{H}_k^{(n)})_k$. □

IV Ordinaux

Pour terminer la partie sur les graphes, nous allons nous intéresser à la réalisation de groupe de cardinal infini, en montrant le théorème établi par Sabidussi dans [10]. Avant de s'intéresser au théorème, il nous faut tout d'abord définir quelques notions que nous utiliserons plus tard.

IV.1 Relations et propriétés

Definition IV.1.1 (Relation) Soient E, F deux ensembles. Une *relation binaire* $\mathcal{R}$ de E sur F est un sous-ensemble $\mathcal{G}$ de $E \times F$. Si $(x, y) \in \mathcal{G}$ on dit que x *est en relation avec* y, noté "$x\mathcal{R}y$".

On appelle *relation interne* une relation binaire d'un ensemble E sur lui-même.

Remarque: Dans la suite, nous n'utiliserons que des relations internes à un ensemble E, ainsi on simplifiera l'appellation en : "*relation* sur E".

Definition IV.1.2 Soit E un ensemble et $\mathcal{R}$ une relation sur E. On dit que $\mathcal{R}$ est *bien fondée* si toute partie non vide X de E possède un élément $\mathcal{R}$-minimal, i.e.

$$\forall X \subset E, \exists m \in X, \forall x \in X, x \not\mathcal{R} m$$

Remarque: En particulier, si $x \in E$, $\{x\} \subset E$ et donc $x \not\mathcal{R} x$.

Cette notion de relation bien fondée nous permet d'introduire l'induction :

Proposition IV.1.3 (Induction) *Soit E un ensemble et $\mathcal{R}$ une relation sur E bien fondée et, soit $\mathcal{P}$ une propriété telle que pour tout x dans E on peut déterminer si $\mathcal{P}(x)$ est vraie ou non (séparabilité). Si, pour tout $x \in E$, si pour tout $y \in E$ tel que $y\mathcal{R}x$, $\mathcal{P}(y)$ est vraie, alors $\mathcal{P}(x)$ est vraie. Alors pour tout $x \in E$, $\mathcal{P}(x)$ est vraie. Plus précisément :*

$$(\forall x \in E, ((\forall y \in E, y\mathcal{R}x \Rightarrow \mathcal{P}(y)) \Rightarrow \mathcal{P}(x))) \Rightarrow \forall x \in E, \mathcal{P}(x)$$

Remarque: Par rapport à la récurrence classique, l'induction ne demande pas une initialisation. Malgré tout, si la propriété "$\forall x \in E, ((\forall y \in E, y\mathcal{R}x \Rightarrow \mathcal{P}(y)) \Rightarrow \mathcal{P}(x))$" est vérifiée, alors si on prend m l'élément $\mathcal{R}$-minimal de E, il n'existe pas d'élément $y \in E$ tel que $y\mathcal{R}m$ ainsi $\mathcal{P}(m)$ est vraie.

Preuve. En reprenant les notations de l'énoncé, on considère :

$$X = \{x \in E \mid \mathcal{P}(x) \text{ n'est pas vrai } \}.$$

Si X n'est pas vide, E étant bien fondé, il existe m un élément $\mathcal{R}$-minimal. Soit $y \in E$ tel que $y\mathcal{R}m$, par minimalité de m on sait que $y \notin X$, donc $\mathcal{P}(y)$ est vraie. Donc, on a que : $\forall y \in E, y\mathcal{R}m \Rightarrow \mathcal{P}(y)$ est vraie, ce qui entraine que $\mathcal{P}(m)$ est vraie. Donc m n'est pas dans X, ce qui est absurde donc X est vide. □

Nous allons vouloir caractériser certaines propriétés de ces relations pour définir la notion d'ordre.

Definitions IV.1.4 Soit E un ensemble et $\mathcal{R}$ une relation sur E. On dit que $\mathcal{R}$ est :

a) *réflexive* si : $\forall x \in$E$, x\mathcal{R}x$.

b) *antiréflexive* si : $\forall x \in$E$, x\not\mathcal{R}x$.

c) *antisymétrique* si : $\forall (x, y) \in E^2, (x\mathcal{R}y \text{ et } y\mathcal{R}x) \Rightarrow x = y$.

d) *transitive* si : $\forall x, y, z \in E, (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.

e) *asymétrique* si : $\forall x, y \in E, x\mathcal{R}y \Rightarrow \text{non}(y\mathcal{R}x)$.

Remarque: L'asymétrie entraine l'antiréflexivité.

IV.2 Ordre

Definition IV.2.1 (Ordre) Soit E un ensemble, un *ordre* sur E est une relation $\mathcal{R}$ sur E qui est réflexive, antisymétrique et transitive. Un *ordre strict* est une relation asymétrique et transitive.

À tout ordre, $\leqslant$ on peut associer son *ordre strict associé* $<$, une autre relation d'ordre stricte définie par :

$$\forall x, y \in E, x < y \Leftrightarrow (x \leqslant y \text{ et } x \neq y)$$

Inversement, à tout ordre strict $<$ on peut associer son ordre large associé $\leqslant$, définie par :

$$\forall x, y \in E, x \leqslant y \Leftrightarrow (x < y \text{ ou } x = y)$$

Definition IV.2.2 (Bon ordre) Un ordre $\leqslant$ sur un ensemble E est dit *bon* si pour toute partie non vide de E possède un plus petit élément (pour $\leqslant$). On dit alors que $(E, \leqslant)$ est un ensemble *bien ordonné*. On dira qu'un ordre strict est un *bon ordre strict* si l'ordre large associé est bon.

Definition IV.2.3 (Total) Soit E un ensemble. Un ordre $\leqslant$ sur E est *totalement* ordonné si :

$$\forall x, y \in E, x \leqslant y \text{ ou } y \leqslant x.$$

De même, on dira qu'un ordre strict est totalement ordonné si son ordre large associé est totalement ordonné.

Lemme IV.2.4 *Pour tout ordre strict $<$ sur E, il y a équivalence entre :*

(i) la relation $<$ est ordre total bien fondé ;

(ii) la relation $<$ est un bon ordre.

Preuve. Supposons que $<$ est un ordre total bien fondé sur E, et soit X une partie non vide de E. On prend donc $m \in X$ tel que pour tout $x \in X$ on a $x \not< m$. Comme $<$ est un ordre total, si $x < m$ n'est pas vrai alors on a $m \leq x$, et donc m est le plus petit élément de X. Donc $<$ est un bon ordre.

Inversement, supposons que $<$ est un bon ordre sur E. Montrons que $<$ est total. En effet, si $a, b \in E$ le sous-ensemble de E, défini par $\{a, b\}$, admet un plus petit élément, donc on a $a \leq b$ ou $b \leq a$. D'autre part, si X est une partie non vide de E alors X possède un plus petit élément et donc pour tout $x \in X$ on a $m \leq x$ donc on a $x \not< m$ et donc m est un élément $<$-minimal pour X et $<$ est une relation bien fondée. □

Remarque: La proposition d'induction pour les relations bien fondées peut être appliquée aux bons ordres stricts.

IV.3 Catégorie sur les ordres

Nous allons enfaite voir qu'il est possible de définir la catégorie des ensembles ordonnés munis des morphismes de la définition IV.3.1. Nous pourrions nous poser également la question de la réalisabilité de groupe de cette catégorie. C'est en fait assez simple de voir que tout groupe d'automorphisme associé à un élément est le groupe trivial. C'est ce que nous allons voir dans la suite.

Definition IV.3.1 Soient A,B deux ensembles et $<, \prec$ deux ordres stricts sur A et, B respectivement. On appelle application *strictement croissante* (ou morphisme d'ensemble ordonné) une application $f : A \to B$ qui vérifie :

$$\forall x, y \in A, x < y \Rightarrow f(x) \prec f(y)$$

Lemme IV.3.2 *Soient $(A, <)$, $(B, \prec)$ deux ensembles ordonnés. Supposons que $<$ est total et que $f : A \to B$ est une application strictement croissante. Alors f est injective et $x < y \leftrightarrow f(x) \prec f(y)$.*

Grâce à ces morphismes, on peut définir la catégorie des ensembles ordonnés Ord. Et donc nous avons les définitions classiques qui s'ensuivent :

Definition IV.3.3 Soient A,B deux ensembles et $<, \prec$ deux ordres stricts sur A et B respectivement. On appelle *isomorphisme* d'ensembles ordonnés une application $f : A \to B$ tel qu'il existe une application $g : B \to A$ strictement croissante telle que :

$$f \circ g = id_B, \quad g \circ f = id_A.$$

Remarque: Les isomorphismes d'ensembles ordonnés sont en fait les applications strictement croissantes et bijectives, car ce sont en particulier des morphismes pour la catégorie Set, donc des bijections.

Notation : Comme dans les autres exemples, on peut donc, pour tout ensemble ordonné, $(A, <)$ définir le groupe d'automorphisme pour cette catégorie, contenant les isomorphismes d'ensembles ordonnés de A dans lui-même. Noté $\mathrm{Aut}_{Ord}(A)$.

Les énoncés suivants répondront à la question de la réalisabilité de groupe pour une sous-catégorie de Ord que l'on notera $bOrd$ qui est la catégorie des ensembles bien ordonnés (les morphismes sont les mêmes, juste restreints aux bons ordres).

Lemme IV.3.4 *Soit $(A, <)$ un ensemble bien ordonné et $f : A \to A$ une application strictement croissante. Alors pour tout $a \in A$, on a $a \leqslant f(a)$.*

Preuve. On pose $X = \{x \in A \mid f(x) < x\}$. Si A est vide, on a le résultat trivialement. Supposons donc maintenant que A est non vide. Supposons maintenant par l'absurde que X est non vide alors X a un plus petit élément que l'on nommera m. Puisque $m \in X$, on a $f(m) < m$. Comme f est strictement croissante, on a : $f(f(m)) < f(m)$. De plus $f(m) < m$, donc $f(m)$ n'est pas dans X car m est l'élément minimal de X. Donc par définition de X : $f(f(m)) \not< f(m)$. On obtient donc une contradiction et X est donc vide. □

Proposition IV.3.5 *Soient $(A, <)$, $(B, \prec)$ deux ensembles bien ordonnés. Il existe au plus un isomorphisme de $(A, <)$ sur $(B, \prec)$. En particulier, l'identité est le seul automorphisme d'un ensemble bien ordonné. Ou encore, les ensembles bien ordonnés sont des éléments rigides pour cette catégorie (*$\mathrm{Aut}_{bOrd}(A) \cong \{id_A\}$*).*

Preuve. Soient f et g deux isomorphismes de $(A, <)$ sur $(B, \prec)$. Étant des ensembles bien ordonnés, par le Lemme IV.2.4, ces ordres sont totaux. On peut donc appliquer le Lemme IV.3.2 à g pour montrer que g^{-1} est strictement croissante.

En effet, soient $(x, y) \in B$ tels que $x \prec y$, comme g est un isomorphisme, c'est en particulier une bijection, donc il existe $(u, v) \in A$ tels que $g(a) = x, g(b) = y$, ainsi $g(a) \prec g(b)$ et par le Lemme, on a $a < b$, c'est-à-dire $g^{-1}(x) < g^{-1}(y)$, donc g^{-1} strictement croissante.

On considère donc $g^{-1} \circ f : A \to A$ qui est aussi une application strictement croissante. Le Lemme IV.3.4 implique donc que pour tout $a \in A$, $a \leqslant g^{-1} \circ f(a)$, on applique donc, à cette égalité, g qui est strictement croissante et on obtient : $\forall a \in A, g(a) \preccurlyeq f(a)$. En inversant le rôle de f et g on peut montrer que l'on a aussi : $\forall a \in A, f(a) \preccurlyeq g(a)$. Donc, on obtient le résultat. □

IV.4 Opérations sur les ordres

Definition IV.4.1 (Somme) 1. Soient A, B deux ensembles. On définit leur *somme disjointe* comme étant :

$$A \uplus B = (A \times \{1\}) \cup (B \times \{2\}).$$

2. Soient $\mathcal{A} = (A, <)$ et $\mathcal{B} = (B, \prec)$ deux ensembles ordonnés. On définit leur *somme* comme étant le couple $\mathcal{A} + \mathcal{B} = (A \uplus B, \sqsubset)$, où $\sqsubset$ est définie par : pour tous $(a, i), (b, j) \in A \uplus B$,

$$(a,i) \sqsubset (b,j) \Leftrightarrow \begin{cases} (i = j = 1 \text{ et } a < b), \text{ ou} \\ (i = j = 2 \text{ et } a \prec b), \text{ ou} \\ (i = 1 \text{ et } j = 2). \end{cases}$$

Definition IV.4.2 (Produit) 1. Soient A, B deux ensembles. On définit leur *produit cartésien* de A et B l'ensemble :

$$A \times B := \{(a, b) \mid a \in A, b \in B\}$$

2. Soient $\mathcal{A} = (A, <)$ et $\mathcal{B} = (B, \prec)$ deux ensembles ordonnés. Leur *produit* est le couple $\mathcal{A} \times \mathcal{B} = (A \times B, \sqsubset)$, où $\sqsubset$ est définie par : pour tous $(a, b), (a', b') \in A \times B$,

$$(a,b) \sqsubset (a',b') \Leftrightarrow (b \prec b') \text{ ou } (b = b' \text{ et } a < a')$$

Definition IV.4.3 (Exponentiation) 1. Soient A, B deux ensembles.
L'ensemble des suites d'éléments de A indexé par B est :

$$A^B := \{(a_b)_{b \in B} \mid \forall b \in B, a_b \in A\}$$

2. Soit $(A, <)$ un ensemble ordonné, B un ensemble. Supposons de plus que $(A, <)$ possède un plus petit élément noté 0. Soit $s = (s_b)_{b \in B}$ une suite de A^B. On appelle le *support* de s l'ensemble $\{b \in B \mid s_b \neq 0\}$. On note $A^{(B)}$ le sous-ensemble de A^B ne contenant que les suites à support fini.
3. Soient $\mathcal{A} = (A, <)$ et $\mathcal{B} = (B, \prec)$ deux ensembles ordonnés. On appelle *exponentiation* de $\mathcal{A}$ par $\mathcal{B}$, et on le note $\mathcal{A}^{\mathcal{B}}$, le couple $(A^{(B)}, \sqsubset)$ où $\sqsubset$ est définie par : pour tous $s = (s_b)_{b \in B}$, $t = (t_b)_{b \in B}$,

$$s \sqsubset t \Leftrightarrow \exists b_0 \in B, s_{b_0} < t_{b_0} \text{ et } \forall b_0 \prec b, s_b = t_b$$

Remarque: Il est possible de montrer que si $\mathcal{A}$ et $\mathcal{B}$ sont des ensembles totalement ordonnés (resp. bien ordonnés) alors les constructions $\mathcal{A} + \mathcal{B}$, $\mathcal{A} \times \mathcal{B}$ et $\mathcal{A}^{\mathcal{B}}$ forment des ensembles totalement ordonnés (resp. bien ordonnés). Pour plus de détails, nous conseillons au lecteur de consulter les notes de cours : [3].

Finalement, avant de passer à la définition d'ordinal, nous énoncerons juste la propriété suivante :

Proposition IV.4.4 *Soient $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{C}$ des ensembles ordonnés.*

- *Il existe un isomorphisme de $(\mathcal{A} + \mathcal{B}) + \mathcal{C}$ sur $\mathcal{A} + (\mathcal{B} + \mathcal{C})$.*
- *Il existe un isomorphisme de $\mathcal{A} \times (\mathcal{B} + \mathcal{C})$ sur $(\mathcal{A} \times \mathcal{B}) + (\mathcal{A} \times \mathcal{C})$.*
- *Il existe un isomorphisme de $\mathcal{A}^{\mathcal{B}+\mathcal{C}}$ sur $\mathcal{A}^{\mathcal{B}} \times \mathcal{A}^{\mathcal{C}}$.*
- *Il existe un isomorphisme de $\mathcal{A}^{\mathcal{B} \times \mathcal{C}}$ sur $(\mathcal{A}^{\mathcal{B}})^{\mathcal{C}}$.*

Preuve. Admis ici, voir la source [3]. □

IV.5 Ordinaux

Definition IV.5.1 (Transitif) Un ensemble d'ensembles E est dit *transitif* si tout élément d'un élément de E est un élément de E, c'est-à-dire si l'ensemble $\bigcup_{y\in E} y$ est inclus dans E. Ou encore si

$$x \in y \in E \Rightarrow x \in E$$

Lemme IV.5.2 *(i) $\emptyset$ est transitif.*

(ii) Si E est un ensemble transitif, $E \cup \{E\}$, $\mathcal{P}(E)$ et $\bigcup_{y\in E} y$ le sont.

(iii) Toute union et toute intersection d'ensembles transitifs est transitive.

Preuve. (i) $\emptyset$ n'a pas d'éléments, donc ces éléments vérifient bien la propriété.

(ii) Soit E un ensemble transitif.
Soient $y \in E \cup \{E\}$ et $x \in y$ alors soit $y \in E$ et donc $x \in E \subset E \cup \{E\}$ ou, soit $y = E$ et $x \in E \subset E \cup \{E\}$.
Soit $y \in \mathcal{P}(E)$ alors $y \subset E$ donc si $x \in y$ alors $x \in E$ et donc $\forall z \in x, z \in E$ i.e. $x \subset E$ donc $x \in \mathcal{P}(E)$.
Soit $y \in \bigcup_{z\in E} z$ alors $y \in E$ donc si $x \in y$ alors $x \in y \in E$ donc $x \in E$ et $x \in \bigcup_{z\in E} z$.

(iii) Soient $(E_i)_{i\in I}$ une famille d'ensembles transitifs.
Soit $y \in \bigcup_{i\in I} E_i$ et, soit $x \in y$ alors il existe $i_0 \in I$ tel que $y \in E_{i_0}$ et donc comme E_{i_0} est transitif on obtient que $x \in E_{i_0} \subset \bigcup_{i\in I} E_i$.

Definition IV.5.3 (Ordinal) On dit qu'un ensemble α est un *ordinal*, si α est un ensemble transitif et que la restriction de $\in$ à α est un bon ordre strict.

Autrement dit, α est un ordinal si les quatre conditions suivantes sont vérifiées :

i) pour tout $x \in \alpha$, on a $x \subseteq \alpha$,

ii) pour tout $x \in \alpha$, on a $x \notin x$,

iii) pour tous $x, y, z \in \alpha$, si on a $x \in y$ et $y \in z$, alors on a $x \in z$,

iv) pour tout $A \subseteq \alpha$, il existe $x \in A$ vérifiant $x \in y$ pour tout $y \in A$ distinct de x.

Propriété IV.5.4 *1. $\emptyset$ est un ordinal*

2. Si α est un ordinal, alors $\alpha \notin \alpha$.

3. Si α est un ordinal, alors $\alpha \cup \{\alpha\}$ en est un aussi.

Preuve. (i) Les 4 propriétés d'un ordinal sont trivialement vérifiées car $\emptyset$ est vide et ne possède aucun sous-ensemble non vide.

(ii) Soit α un ordinal. Par définition d'ordinal, pour tout x dans α, on a $x \notin x$, mais donc si $\alpha \in \alpha$ alors $\alpha \notin \alpha$. Ce qui est absurde, donc $\alpha \notin \alpha$.

(iii) Soit α un ordinal. α est en particulier un ensemble transitif et donc le Lemme IV.5.2 affirme que $\beta := \alpha \cup \{\alpha\}$ est aussi un ensemble transitif, il vérifie donc la propriété (i) de la Définition IV.5.3 d'ordinal. Vérifions les autres points.
Soit $x \in \beta$. Comme $\beta = \alpha \cup \{\alpha\}$, on a ou bien $x \in \alpha$, ou bien, $x = \alpha$ car on ne peut pas avoir les deux par le point (*2*) de la Propriété. Dans le premier

cas, par définition de α ordinal $x \in x$, dans le second cas, on a $x = \alpha \notin \alpha = x$, toujours par (*2*). C'est donc le point (ii) de la Définition.

Soient $x, y, z \in \beta$ tels que $x \in y$ et $y \in z$. Si $x, y, z \in \alpha$, alors on a $x \in z$ par définition de α ordinal. Supposons par l'absurde que $x = \alpha$. Par (*2*), on ne peut pas avoir $y = \alpha$, donc $\alpha \in y \in \alpha$, ce qui est absurde, donc $x \in \alpha$. Supposons par l'absurde maintenant que $y = \alpha$, comme précédemment, on a que $z \neq \alpha$, donc $\alpha = y \in z \in \alpha$, ce qui est absurde, donc $y \in \alpha$. Il nous reste donc à voir le cas $z = \alpha$, on a donc $x \in y \in \alpha$, et comme α est transitif $x \in \alpha = z$. On a donc montré le point (iii) de la Définition.

Soit A un sous-ensemble non vide de β. On commence d'abord par étudier le cas $A \cap \alpha \neq \emptyset$. En appliquant le point (iv) de la définition d'ordinal à α, on a qu'il existe $x \in A \cap \alpha$ tel que $x \in y$ pour tout $y \in A \cap \alpha$ distinct de x. Puisque $x \in A \cap \alpha$, on a $x \in \alpha$ et donc pour tout $y \in A$ distinct de x, si $y \in \alpha$, alors on a déjà vu que $x \in y$, sinon $y \notin \alpha$, mais comme $y \in \beta$, $y = \alpha$ ce qui donne $x \in y = \alpha$. Dans le cas où $A \cap \alpha = \emptyset$, comme $A \subset \beta = \alpha \cup \{\alpha\}$, la seule possibilité est $A = \{\alpha\}$. On peut donc poser $x = \alpha$ et il vérifie bien la propriété, car il n'existe pas d'éléments différents de x dans A. On obtient donc le point (iv) de la Définition.

Donc $\beta = \alpha \cup \{\alpha\}$ est un ordinal. □

Ce Lemme nous permet donc d'exhiber un grand nombre d'ordinaux avec la définition suivante :

Definition IV.5.5 L'application *successeur* est l'application qui à un ensemble A renvoie $S(A) := A \cup \{A\}$. On peut donc définir les "*n premiers*" ordinaux grâce à $\emptyset$: pour tout $n \in \mathbb{N}$,

$$\underline{n} := S^n(\emptyset).$$

On peut étudier un peu ces ordinaux $\underline{n}$ grâce à la propriété suivante :

Propriété IV.5.6 *Pour tout entier n, l'ordinal $\underline{n}$ a exactement n éléments qui sont les ordinaux $\underline{k}$ pour $k < n$.*

Preuve. Procédons par récurrence sur $n \in \mathbb{N}$.

- Pour $n = 0$, $\underline{n} = \underline{0} = \emptyset$, le résultat est trivialement vrai.
- Soit $n > 0$, supposons avoir montré le résultat pour $m := n - 1$. On a donc $\underline{n} = S(\underline{m}) = \underline{m} \cup \{\underline{m}\}$. De plus, par la Propriété IV.5.4 on a que $\underline{m} \notin \underline{m}$, ainsi $\underline{n}$ a $n = 1 + n + 1$ éléments qui sont les $\underline{m}$ pour $m < n - 1$ ou $m = n - 1$, c'est-à-dire $m < n$.

On en déduit le résultat par récurrence. □

Remarque: Il existe bien d'autres ordinaux que ceux de la forme $\underline{n}$.

Finalement, nous allons voir des résultats valables sur tous les ordinaux.

Lemme IV.5.7 *Soit $(A, <)$ un ensemble bien ordonné. Si B est un sous-ensemble de A, alors la restriction de $<$ à B ($<_{|_B}$) est un bon ordre.*

Preuve. Si X est une partie non vide de B, alors X a dans A un plus petit élément a pour $<$, et donc $a \in X \subset B$, donc a est le plus petit élément de X pour $(B, <_{|_B})$.□

Proposition IV.5.8 *Tout élément d'un ordinal α est un ordinal strictement inclus dans α.*

Preuve. Soit α un ordinal et $x \in \alpha$. Comme α est transitif, $x \in \alpha$ implique $x \subset \alpha$ et on sait qu'il n'y a pas égalité par le Lemme IV.5.4 (*2*). On veut montrer que x est un ordinal, pour cela nous allons utiliser la caractérisation des ordinaux en tant qu'ensemble transitif et tel que la restriction de $\in$ à α est un bon ordre strict.

Montrons d'abord qu'il est transitif : Soient $z \in y \in x$. Comme $x \subset \alpha$, on déduit $y \in \alpha$ et même $z \in \alpha$ car α est transitif. Par la définition de α en tant qu'ordinal et le fait que $x, y, z \in \alpha$ avec $z \in y \in x$, on a $z \in x$, donc x est transitif.

Pour montrer que $\in_{|_x}$ est un bon ordre, on utilise le Lemme IV.5.7.

Donc x est un ordinal. □

Proposition IV.5.9 *Si A est un ensemble non vide d'ordinaux, $\bigcap A := \bigcap_{x \in A} x$ est un ordinal.*

Preuve. On pose $a := \bigcap A = \{\beta \mid \forall \alpha \in A, \beta \in \alpha\}$. Tout élément de A est un ordinal, donc est transitif, on applique le Lemme IV.5.2 (iii) pour obtenir que a est transitif. Soit α un élément quelconque de A, tout élément de a est un élément de α, donc un ordinal par la propriété IV.5.8. On peut voir que $\in_{|_a}$ est un ordre strict. En effet, soient β, γ, δ des éléments de a, donc de α, par le Lemme IV.5.4 (*2*), on a $\beta \notin \beta$ donc $\beta \in \gamma$, ce qui donne $\gamma \notin \beta$ sinon $\beta \in \beta$ ce qui est absurde, donc $\in_{|_a}$ est asymétrique. Et comme α est un ordinal et $\beta \in \gamma \in \delta$ des éléments de α on a que $\beta \in \delta$ donc $\in_{|_a}$ est aussi transitive, donc $\in_{|_a}$ est un ordre strict. Finalement montrons $\in_{|_a}$ est un bon ordre, pour cela on utilise le Lemme IV.5.7. Soit X une partie non vide de a, c'est en particulier une partie non vide de α, donc elle possède un plus petit élément β par rapport à $\in_{|_\alpha}$ et $\in_{|_\alpha |_a} = \in_{|_a}$ donc comme les éléments de X sont des éléments de a on en déduit aussi que β est un plus petit élément par rapport à $\in_{|_a}$. Donc la relation $\in_{|_a}$ est un bon ordre et a est un ordinal. □

Remarque: On peut définir un ordre sur les ordinaux défini par : si α,β sont deux ordinaux alors $\alpha < \beta$ si $\alpha \in \beta$.

De cette définition d'ordre, on peut déduire une proposition importante pour l'étude des ordinaux.

Proposition IV.5.10 (i) *Tout ordinal coïncide avec l'ensemble contenant tous les ordinaux strictements plus petits que lui.*

(ii) *L'ordre large associé à la restriction de $\in$ aux ordinaux est l'inclusion : si α,β sont des ordinaux, $\alpha \subseteq \beta$ si et seulement on a soit $\alpha \in \beta$, soit $\alpha = \beta$ (i.e. $\alpha \leqslant \beta$).*

(iii) *Pour chaque ordinal α, l'ordinal $S(\alpha)$ est successeur immédiat de α : $\alpha < S(\alpha)$ et $\alpha < \beta$ entraine $S(\alpha) \leqslant \beta$. De plus S est strictement croissante sur les ordinaux.*

Preuve. Soient α,β deux ordinaux.

(i) Le Lemme IV.5.8 donne que α est l'ensemble de ses éléments qui sont des ordinaux, i.e. l'ensemble des ordinaux plus petit que lui par la définition de l'ordre.

(ii) Si on a $\alpha \leqslant \beta$. Alors ou bien $\alpha < \beta$ i.e. $\alpha \in \beta$ i.e. $\alpha \subseteq \beta$ car β est transitif, ou bien $\alpha = \beta \subseteq \beta$.

Réciproquement, supposons $\alpha \subseteq \beta$. On a soit $\alpha = \beta$ et donc $\alpha \leqslant \beta$, soit $\alpha \subseteq \beta$. Dans ce cas $\beta \smallsetminus \alpha$ est une partie non vide de β et, comme $(\beta, \in_{|\beta})$ est bien ordonné, $\beta \smallsetminus \alpha$ admet un plus petit élément α', qui est un ordinal comme tout élément de β. On veut montrer $\alpha = \alpha'$, qui donne $\alpha = \alpha' \in \beta$, donc $\alpha < \beta$ et en particulier $\alpha \leqslant \beta$.

Montrons que $\alpha' = \alpha$. Raisonnons par double inclusion. Soit $\gamma \in \alpha$. Puisque $\alpha \subseteq \beta$, on a $\gamma \in \beta$ et donc on a l'un des relations suivantes : $\gamma \in \alpha'$, $\gamma = \alpha'$, $\alpha' \in \gamma$. Mais $\gamma = \alpha'$ donnerait $\gamma \notin \alpha$ car α' est dans $\beta \smallsetminus \alpha$, ce qui est absurde. De même, $\alpha' \in \gamma$ entraînerait, par transitivité de α, $\alpha' \in \alpha$ ce qui est absurde par $\alpha' \in \beta \smallsetminus \alpha$. Donc, on a $\gamma \in \alpha'$ i.e. $\alpha \subseteq \alpha'$.

Inversement, soit $\gamma \in \alpha'$. Comme β est transitif, cela donne $\gamma \in \beta$ et la définition de α' comme plus petit élément de $\beta \smallsetminus \alpha$ empêche γ d'être dans $\beta \smallsetminus \alpha$, donc $\gamma \in \alpha$. On a que la double inclusion et $\alpha = \alpha'$.

(iii) $\alpha \in \alpha \cup \{\alpha\} = S(\alpha)$ donc $\alpha < S(\alpha)$. Supposons que l'on a $\alpha < \beta$, on a alors $\alpha \in \beta$ et même $\{\alpha\} \subseteq \beta$. Mais $\alpha < \beta$ implique aussi $\alpha \leqslant \beta$, donc par le point (ii), $\alpha \subseteq \beta$. Si on regroupe, cela donne $\alpha \cup \{\alpha\} \subseteq \beta$, en appliquant toujours le point (ii), $S(\alpha) \leqslant \beta$. Finalement pour la décroissance, on a : $\alpha < \beta$ entraîne $S(\alpha) \leqslant \beta < S(\beta)$. □

L'ordre sur les ordinaux est un bon ordre :

Proposition IV.5.11 *Tout ensemble non vide d'ordinaux A possède un plus petit élément, à savoir $\bigcap A$.*

Preuve. On rappelle que $\alpha = \bigcap A := \bigcap_{x \in A} x$. Par la Proposition IV.5.9 on sait que $\bigcap A$ est un ordinal. On sait que $\forall \beta \in A$, $\alpha \subseteq \beta$ et donc par la Proposition IV.5.10 (ii), on obtient que $\alpha \leqslant \beta$. Supposons par l'absurde que, pour tout $\beta \in A$, $\alpha < \beta$ (i.e. qu'il n'existe pas d'éléments dans A qui soit α), c'est-à-dire $\alpha \in \beta$. Ceci étant valable pour tout $\beta \in A$, on a que $\alpha \in \bigcap A = \alpha$, ce qui est absurde par la Propriété IV.5.4 (*2*). Donc il existe $\beta \in A$ tel que $\beta = \alpha = \bigcap A$, donc $\bigcap A \in A$ est un élément minimal. □

En appliquant ce résultat à $\{\alpha, \beta\}$, on a :

Corrolaire IV.5.12 *Soient α, β deux ordinaux. Alors, on a une des trois relations suivantes :*

— $\alpha \in \beta$,

— $\alpha = \beta$,

— $\beta \in \alpha$.

Il est important de vérifier si l'on peut faire une induction sur les ordinaux.

Proposition IV.5.13 (Induction) *Soit $\mathcal{P}$ une propriété qui vérifie que, pour tout ordinal α on peut déterminer si $\mathcal{P}(\alpha)$ est vraie ou non (séparabilité).*

(i) *Soit θ un ordinal. Si pour tout $\alpha < \theta$, la propriété $\mathcal{P}(\alpha)$ est vraie dès que pour tout $\beta < \alpha$, $\mathcal{P}(\beta)$ est vraie. Alors $\mathcal{P}(\alpha)$ est vraie pour tout ordinal α plus petit que θ.*

(ii) *Supposons que $\mathcal{P}(\alpha)$ est vraie dès que $\mathcal{P}(\beta)$ l'est pour $\beta < \alpha$. Alors $\mathcal{P}$ est vérifiée pour tout ordinal α.*

Preuve. (i) Ce point découle de la Proposition IV.1.3 appliqué à l'ensemble bien ordonné $(\theta, <)$.

(ii) Supposons comme dans l'énoncé que $\mathcal{P}(\alpha)$ est vraie dès que $\mathcal{P}(\beta)$ l'est pour $\beta < \alpha$ et qu'il existe α ordinal tel que $\mathcal{P}(\alpha)$ soit fausse. On pose $X := \{\beta \in \alpha \mid \mathcal{P}(\beta) \text{ est fausse}\}$ qui est bien défini par l'hypothèse de séparabilité de $\mathcal{P}$ (il y a enfaite ici un problème sur la définition de séparabilité, mais admettons que tout se passe bien). En appliquant la contraposée du point (i), on a que X est non vide, il admet donc un plus petit élément γ. Alors $\mathcal{P}(\gamma)$ est fausse et γ étant minimum on a qu'il n'existe pas d'élément plus petit que γ tel que la propriété soit fausse. Ce qui est absurde, car en appliquant le point (i) à γ on obtient que $\mathcal{P}(\gamma)$ est vraie. Ainsi il n'existe pas d'ordinal α tel que $\mathcal{P}(\alpha)$ soit fausse. □

Definition IV.5.14 (Borne supérieure) Soit A un ensemble d'ordinaux. Nous allons définir $\bigcup A := \bigcup_{x \in A} x$.

Definition IV.5.15 (Ordinal limite, successeur) Un ordinal α est appelé un *successeur* (resp. *limite*) s'il existe, β vérifiant $\alpha = S(\beta)$ (resp. si α est distinct de $\underline{0}$ et vérifie $\alpha = \bigcup \alpha$).

Proposition IV.5.16 *Tout ensemble d'ordinaux A possède une borne supérieure, à savoir $\bigcup A$.*

Preuve. Admis ici, voir la source [3]. □

Proposition IV.5.17 *Pour tout ordinal α, on a la disjonction :*

— *ou bien $\beta < \alpha$ entraîne $S(\beta) < \alpha$ pour tout β, et on a alors $\bigcup \alpha = \alpha$.*

— *ou bien il existe β tel qu'on ait $\alpha = S(\beta)$, et on a alors $\bigcup \alpha = \beta$.*

Preuve. Soit α un ordinal, α est un ensemble transitif donc on a $\bigcup \alpha \subseteq \alpha$. De plus $\bigcup \alpha$ est un ordinal par la Proposition IV.5.16, et donc par la Proposition IV.5.10 (ii), $\bigcup \alpha \leqslant \alpha$. De plus, si on a $\beta < \alpha$, par la Proposition IV.5.10 (iii) on a que $S(\beta) \leqslant \alpha$. On a donc deux cas :

Ou bien $S(\beta) < \alpha$ pour tout $\beta < \alpha$, et alors $\beta < S(\beta) < \alpha$ et donc $\beta \in S(\beta) \in \alpha$, et donc $\beta \in \bigcup \alpha$, et finalement étant valable pour tout $\beta < \alpha$, $\alpha \subseteq \bigcup \alpha$, ainsi on a égalité $\alpha = \bigcup \alpha$.

Ou bien, il existe $\beta_0 < \alpha$ tel que $S(\beta_0) \geqslant \alpha$, et donc on a l'égalité $S(\beta_0) = \alpha$. Dans ce cas $\gamma < \beta$ entraîne $\gamma \in \beta \in \alpha$, donc encore une fois, $\gamma \in \bigcup \alpha$, cette relation étant valable pour tout $\gamma < \beta$, on a $\beta \in \bigcup \alpha$. Et d'un autre côté on a : $\bigcup \alpha = \bigcup(S(\beta)) = \bigcup(\beta \cup \{\beta\}) = (\bigcup \beta) \cup \beta \subseteq \beta$, on a donc l'égalité $\bigcup \alpha = \beta$. □

Proposition IV.5.18 *Tout ensemble A bien ordonné est isomorphe à un unique ordinal α.*

Preuve. Admis ici, voir la source [3]. □

IV.6 Arithmétique ordinale

Definition IV.6.1 (Segment initial) Soit $<$ un ordre sur A et $a \in A$, on appelle *segment initial* de $(A, <)$ déterminé par a, l'ensemble :

$$I_<(a) := \{x \in A \mid x < a\},$$

muni de l'ordre induit par $<$.

Le lemme suivant nous permet de facilement construire les relations d'ordre entre les ordinaux.

Lemme IV.6.2 *Soient α, β deux ordinaux qui sont respectivement isomorphes aux ensembles bien ordonnés $\mathcal{A}$ et $\mathcal{B}$.*

(i) Pour avoir $\alpha = \beta$, il suffit de construire une bijection strictement croissante de $\mathcal{A}$ sur $\mathcal{B}$.

(ii) Pour avoir $\alpha < \beta$, il suffit de construire une bijection strictement croissante de $\mathcal{A}$ sur un segment initial de $\mathcal{B}$.

(iii) Pour avoir $\alpha \leqslant \beta$, il suffit de construire une injection strictement croissante de $\mathcal{A}$ sur $\mathcal{B}$.

Preuve. (i) Ce point vient simplement de l'unicité de la Proposition IV.5.18.

(ii) L'existence d'un tel isomorphisme entraine l'existence d'un morphisme de $(\alpha, <)$ sur un segment initial de $(\beta, <)$, qui eux, sont déterminés par des éléments $\gamma \in \beta$ et le segment initial associé coïncide avec γ. On a donc $\alpha = \gamma < \beta$.

(iii) Avec le présupposé de l'énonce, on a une injection croissante f de $(\alpha, <)$ dans $(\beta, <)$. Si on avait $\beta < \alpha$, alors l'application f serait une injection croissante de $(\beta, <)$ dans un de ses segments initiaux $\gamma < \beta$, ce qui contredit le Lemme IV.3.4 (ou plutôt sa démonstration réécrite pour les ordinaux). Donc $\beta < \alpha$ est faux, et comme l'ordre sur les ordinaux est un ordre total, la seule possibilité est $\alpha \leqslant \beta$. □

On peut donc définir les opérations :

Definition IV.6.3 (Addition) Soient α, β deux ordinaux, on définit leur *somme*, comme l'unique ordinal γ tel que $(\gamma, \in)$ soit isomorphe à $(\alpha, \in) + (\beta, \in)$ (en tant qu'ensembles ordonnés).

Remarque: On peut faire plusieurs remarques, les démonstrations ne seront pas faites mais, nous utiliseront, sans les plébisciter, ces résultats à l'avenir.

— Soient $n, k \in \mathbb{N}$, $\underline{n} + \underline{k} = \underline{n+k}$.

— Si ω est un ordinal limite, $\underline{1} + \omega = \omega = \omega + \underline{0}$. ⚠ Par contre, on a $\underline{1} \neq \underline{0}$ ainsi, on voit qu'on ne peut pas simplifier sans faire attention.

— Soit α un ordinal quelconque, $\alpha + \underline{0} + \underline{0} + \alpha = \alpha$; $\alpha + \underline{1} = S(\alpha)$ et :

$$\underline{1} + \alpha = \begin{cases} S(\alpha) & \text{si } \alpha \text{ fini,} \\ \alpha & \text{si } \alpha \text{ infini.} \end{cases}$$

— L'addition ordinale est associative.

Definition IV.6.4 (Multiplication) Soient α, β deux ordinaux, on définit $\alpha.\beta$ comme l'unique ordinal γ tel que $(\gamma, \in)$ soit isomorphe à $(\alpha, \in) \times (\beta, \in)$.

Remarque: Comme précédemment pour l'addition, on peut lister arbitrairement certaines propriétés utiles :

— Soient $n, k \in \mathbb{N}$, $\underline{n}.\underline{k} = \underline{n.k}$.

— Soit ω un ordinal limite, $\underline{2}.\omega = \omega$.

— Soit α un ordinal quelconque et $n \in \mathbb{N}$. On a : $\alpha.\underline{0} = \underline{0}.\alpha = \underline{0}$; $\underline{1}.\alpha = \alpha.\underline{1} = \alpha$; $\alpha.\underline{n} = \alpha + \cdots + \alpha$.

— La multiplication ordinale est associative et distributive à gauche par rapport à l'addition.

Definition IV.6.5 (Exponentiation) Soient α, β deux ordinaux. On définit α^β comme l'unique ordinal γ tel que $(\gamma, \in)$ soit isomorphe à $(\alpha, \in)^{(\beta, \in)}$.

Remarque: Encore une fois, quelques propriétés :

— Soient $n, k \in \mathbb{N}$, $\underline{n}^{\underline{k}} = \underline{n^k}$.

— Soit α un ordinal quelconque. On a : $\alpha^{\underline{0}} = \underline{1}$; $\alpha^{\underline{1}} = \alpha$; $\underline{1}^\alpha = \underline{1}$ et $\underline{0}^\alpha = \underline{0}$ si $\beta \neq \underline{0}$.

— Soient α, β, γ trois ordinaux, on a : $\alpha^{\beta+\gamma} = \alpha^\beta.\alpha^\gamma$ et $\alpha^{\beta.\gamma} = (\alpha^\beta)^\gamma$.

Finalement, pour une étude plus détaillée de toutes les propriétés associées aux opérations définies ci-dessus, le lecteur pourra, encore une fois, se référer à la source [3].

IV.7 Equipotents

Finissons ce paragraphe avec des propriétés sur les équipotents qui serviront dans la démonstration de l'énoncé de la partie suivante.

Definition IV.7.1 (Équipotents) Soit E, F deux ensembles, ont dit qu'ils sont équipotents s'il existe une bijection de E dans F.

Théorème IV.7.2 *Soit E un ensemble de cardinalité infinie, on a une bijection entre E et $E \times E$.*

Lemme IV.7.3 *Soit E un ensemble de cardinalité infinie contient un ensemble équipotent à $\mathbb{N}$.*

Preuve (Lemme IV.7.3). Soit $a_0 \in E$, pour tout $n \in \mathbb{N}$ on prend $a_n \in E \setminus \{a_0, ..., a_{n-1}\} \neq \emptyset$. On pose $D = \{a_i \mid i \in \mathbb{N}\} \subset E$ ainsi l'application :

$$\begin{array}{ccc} \mathbb{N} & \to & D \\ n & \mapsto & a_n, \end{array}$$

est une bijection de $\mathbb{N}$ dans un sous-ensemble de E, $D \subset E$ équipotent à $\mathbb{N}$. □

Lemme IV.7.4 $\mathbb{N} \times \mathbb{N}$ *équipotent à* $\mathbb{N}$.

Preuve (Lemme IV.7.4). On définit

$$h : \begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \\ (a, b) & \mapsto & 2^a(2b+1), \end{array}$$

- Surjectivité : Soit $n \in \mathbb{N}$. On pose $a = \max\{k \geq 0 \mid 2^k \text{ divise } n\}$, alors $n/2^a$ est impair donc il existe $b \in \mathbb{N}$, tel que $n/2^a = 2b + 1$ et donc $h(a, b) = n$.
- Injectivité : Soient $a, b, c, d \in \mathbb{N}$, tels que $h(a, b) = h(c, d)$ ainsi $2^a(2b + 1) = 2^c(2d+1)$. On peut supposer sans perte de généralité que $a \geq c$, alors $2^{a-c}(2b+1) = 2d + 1$ impair donc $a - c = 0$, il suit que $a = c$ et ensuite $b = d$.

On a donc le résultat. □

Avant de passer à la démonstration du Théorème, on rappelle le Lemme de Zorn.

Definition IV.7.5 (Inductif) Soit $(E, <)$ un ensemble ordonné. On dit que E est *inductif* si toute partie de E totalement ordonnée admet un majorant.

Lemme IV.7.6 (Zorn) *Tout ensemble inductif admet un élément maximal.*

Preuve (Théorème IV.7.2). On note $\mathfrak{a} = Card(E)$ et on prend $D \subset E$ une partie équipotente à $\mathbb{N}$ obtenue dans le lemme IV.7.3. On sait qu'il existe une bijection $\psi_0 : D \to D \times D$ par le lemme IV.7.4. On définit :

$$\mathfrak{M} = \{(X, \psi) \mid D \subset X \subset E, \psi : X \to X \times X \text{ bijection}, \psi_{|_D} = \psi_0\},$$

et ensuite la relation d'ordre :

$$(X_1, \psi_1) \leq (X_2, \psi_2) \Leftrightarrow X_1 \subset X_2 \text{ et } \psi_{2|_{X_1}} = \psi_1$$

On vérifie simplement que cette relation d'ordre rend $\mathfrak{M}$ inductif. Le Lemme IV.7.6 de Zorn nous indique donc qu'il existe un élément (F, f) dans $\mathfrak{M}$ un élément maximal pour cette relation d'ordre. Supposons par l'absurde que $Card(F) = \mathfrak{b} < \mathfrak{a}$, on sait que $\aleph_0 \leqslant \mathfrak{b}$ et par ce qu'on a vu sur les ordinaux précédemment, on a $\mathfrak{b} \leq 2\mathfrak{b} \leq 3\mathfrak{b} \leq \mathfrak{b}^2 = \mathfrak{b}$ et, $Card(E \setminus F) > \mathfrak{b}$ car sinon, comme $E = (E \setminus F) \cup F$ on a $\mathfrak{a} \leq 2\mathfrak{b} = \mathfrak{b}$, mais c'est impossible car $\mathfrak{b} < \mathfrak{a}$. On peut donc prendre $Y \subset E \setminus F$ équipotent à F, on pose ensuite $Z = F \cup Y$. On veut montrer qu'il existe une bijection $g : Z \to Z \times Z$. On a en effet :

$$Z \times Z = (F \times F) \cup (F \times Y) \cup (Y \times F) \cup (Y \times Y),$$

réunion d'ensembles disjoints et comme F et Y sont équipotents on a :

$$Card(F \times Y) = Card(Y \times F) = Card(Y \times Y) = \mathfrak{b}^2 = \mathfrak{b},$$

et ainsi,

$$Card((F \times Y) \cup (Y \times F) \cup (Y \times Y)) = 3\mathfrak{b} = \mathfrak{b}.$$

On peut donc exhiber une application $f_1 : Y \to (F \times Y) \cup (Y \times F) \cup (Y \times Y)$ bijective, on pose donc :

$$g : \begin{array}{ccl} Z & \to & Z \times Z \\ x & \mapsto & f(x), \text{ si } x \in F, \\ x & \mapsto & f_1(x), \text{ si } x \in Y, \end{array}$$

Mais on a que $g_{|_D} = f_{|_D} = \psi_0$ donc $(Z, g) \in \mathfrak{M}$ et $(F, f) \leq (Z, g)$ et $(F, f) \neq (Z, g)$ ce qui est absurde par maximalité de (F, f). Donc, on a bien $\mathfrak{b} = \mathfrak{a}$, donc il existe un sous-ensemble de E que l'on notera A tel que $Card(A) = \mathfrak{a}$ et une bijection $\alpha : A \to A \times A$. Comme $Card(A) = \mathfrak{a} = Card(E)$, il existe une bijection $\beta : A \to E$ et donc $(\beta, \beta) \circ \alpha \circ \beta^{-1} : E \to E \times E$ bijection. □

V Graphes infini

Le but de cette section est de montrer le Théorème suivant.

Théorème V.0.1 (Sabidussi) *Soit G un groupe et $\mathfrak{a}$ un cardinal. Il existe un graphe X tel que* $\mathrm{Aut}_{Graph}(X) \cong G$.

Pour cela, nous souhaitons raisonner de la même façon que pour le Théorème III.5.1 de Frucht en cardinalité finie, mais avec un groupe de cardinal arbitraire, nous devons introduire une famille assez grande de graphes distincts connexes avec un groupe d'automorphisme trivial (idéalement autant de graphe que la cardinalité). Pour faire cette construction, nous allons montrer le Lemme suivant :

Lemme V.0.2 *Soit $\mathcal{A}$ une famille composée d'ordinaux. À chaque $\alpha \in \mathcal{A}$ on peut associer H_α un graphe tel que la famille $(H_\alpha)_{\alpha \in \mathcal{A}}$ vérifie : pour tous $\alpha, \beta \in \mathcal{A}$ tel que $\alpha \neq \beta$,*

(i) H_α est connecté,

(ii) $\mathrm{Aut}_{Graph}(H_\alpha) \cong \{1\}$,

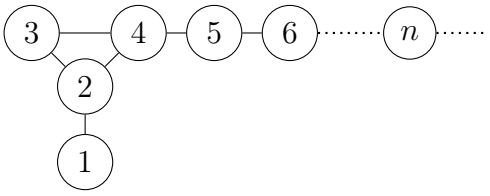
(iii) H_α et H_β ne sont pas isomorphes.

De plus, tout sommet de degré 2 dans ces graphes a pour voisins des sommets de degré inférieur ou égal à $\aleph_0$.

Preuve (Lemme). Commençons par créer un graphe H_0, dénombrable donc son cardinal $\aleph_0$, connecté avec $\mathrm{Aut}_{Graph}(H_0) \cong \{id\}$. Pour cela on peut poser :

$$\begin{aligned} V_{H_0} &= \mathbb{N}, \\ E_{H_0} &= \{[1,2],[2,3],[2,4],[3,4]\} \cup \{[n, n+1] \mid n \in \mathbb{N} \setminus [\![0,3]\!]\}. \end{aligned}$$

Pour obtenir le graphe que l'on peut représenter de la façon suivante :



C'est un graphe connexe, dénombrable et on a déjà vu dans le corollaire du théorème de Frucht que ce genre de construction vérifie $\mathrm{Aut}_{Graph}(H_0) \cong \{id\}$.

Pour obtenir, $H_\alpha, \alpha > 0$ on précède de la manière suivante. On définit tout d'abord la famille de cardinaux indexée sur les ordinaux $(\mathfrak{a}_\alpha)_\alpha$, telle que :

$$\mathfrak{a}_0 = \aleph_0; \forall \alpha > 0, \mathfrak{a}_\alpha = \begin{cases} 2^{\mathfrak{a}_{\alpha-1}} \text{ si } \alpha \text{ n'est pas un ordinal limite,} \\ \sum_{\xi<\alpha} \mathfrak{a}_\xi \text{ sinon.} \end{cases}$$

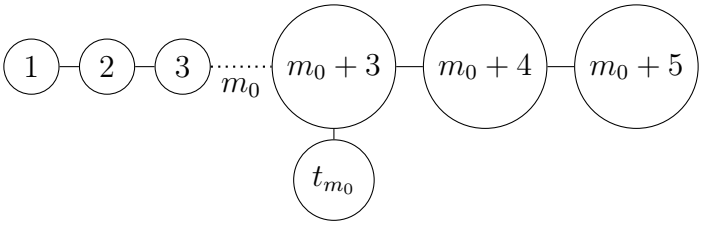
On définit également une famille d'ensemble indexé par les ordinaux $(M_\alpha)_\alpha$ tel que :

$$M_0 = \mathbb{N}; \forall \alpha > 0, M_\alpha = \begin{cases} 2^{M_{\alpha-1}} \text{ si } \alpha \text{ n'est pas un ordinal limit,} \\ \bigcup_{\xi<\alpha} M_\xi \text{ sinon.} \end{cases}$$

où la notation "2^M" si M est un ensemble désigne l'ensemble des applications de M dans $\{0,1\}$: $\mathcal{F}(M, \{0,1\})$, ou l'ensemble des parties de M : $\mathcal{P}(M)$, qui sont des constructions en bijection. On peut donc remarquer que pour tout α la cardinalité de M_α est $\mathfrak{a}_\alpha$. On peut également supposer, en faisant la bonne identification, que pour tout $\xi < \eta$, $M_\xi \subset M_\eta$.

Soit $m_0 \in M_0$, on définit $H_{m_0} = (V(H_{m_0}), E(H_{m_0}))$ de la façon suivante :

$$V(H_{m_0}) = \{1, ..., m_0 + 5, t_{m_0}\}, t_{m_0} \notin M_0,$$
$$E(H_{m_0}) = \{[i, i+1] \mid 1 \leq i \leq m_0 + 4\} \cup \{[m_0 + 3, t_{m_0}]\}.$$



On a que H_{m_0} est connecté et $\mathrm{Aut}_{Graph}(H_{m_0}) \cong \{id\}$, car le sommet m_0+3 est envoyé sur lui-même par un automorphisme, car c'est le seul de degré 3 et toutes les branches connectées à ce sommet sont différentes longueurs donc sont aussi stabilisées par un automorphisme, ainsi le seul automorphisme de H_{m_0} est id. On a donc une famille $(H_{m_0})_{m_0 \in M_0}$ de graphes et si $m_0^1, m_0^2 \in M_0, m_0^1 \neq m_0^2$, alors $H_{m_0^1}$ et $H_{m_0^2}$ n'ont pas le même nombre de sommets donc ne sont pas isomorphes.

Supposons par induction que pour tout $\xi < \alpha$ et tout $m_\xi \in M_\xi$ on a déjà défini le graphe H_{m_ξ} avec les propriétés suivantes sur la famille $(H_{m_\xi})_{\xi<\alpha, m_\xi \in M_\xi}$: pour tous $\xi, \eta < \alpha$ et pour tous $m_\xi, \widehat{m_\xi} \in M_\xi$, $m_\eta \in M_\eta$,

1. H_{m_ξ} est connecté.

2. Si ξ n'est pas un ordinal limite, tous les sommets de H_{m_ξ} sont de degré au plus $\mathfrak{a}_{\xi-1}$ et il existe un sommet de degré $\mathfrak{a}_{\xi-1}$.
   Si ξ est un ordinal limite alors le graphe possède un unique sommet de degré α, les autres sont de degré inférieur.
3. $\mathrm{Aut}_{Graph}(H_{m_\xi}) \cong \{id\}$
4. Si $m_\xi \neq \widehat{m_\xi}$, H_{m_ξ} et $H_{\widehat{m_\xi}}$ ne sont pas isomorphes.
5. Si $\eta \neq \xi$, H_{m_ξ} et H_{m_η} ne sont pas isomorphes.

Soit $m_\alpha \in M_\alpha$, on définit H_{m_α} comme ce qui suit. Soit N_α un ensemble de cardinal $\mathfrak{a}_\alpha$ tel que $M_\alpha \cap N_\alpha = \emptyset$, et, soit $f_\alpha : M_\alpha \to N_\alpha$ une fonction injective. On sépare ensuite la construction en fonction de si α est un ordinal limite ou non :

— Cas 1 : α n'est pas un ordinal limite. On pose :

$$V(H_{m_\alpha}) = \{t_{m_\alpha}\} \cup \left(\bigcup_{m_{\alpha-1} \in M_{\alpha-1}} W_{m_{\alpha-1}} \right),$$

où

$$W_{m_{\alpha-1}} = \begin{cases} (\{m_{\alpha-1}\} \times V(H_{m_{\alpha-1}})) \cup \{(f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}})\} & \text{si } m_{\alpha-1} \in m_\alpha \\ \{(m_{\alpha-1}, t_{m_{\alpha-1}})\} \cup (\{f_{\alpha-1}(m_{\alpha-1})\} \times V(H_{m_{\alpha-1}})) & \text{si } m_{\alpha-1} \notin m_\alpha, \end{cases}$$

et : $\forall \xi < \alpha, \forall m_\xi \in M_\xi, t_{m_\alpha} \notin W_{m_\xi}$ et $t_{m_{\alpha-1}} \in V(H_{m_{\alpha-1}})$ est le sommet qui avait été défini dans la définition de $H_{m_{\alpha-1}}$.

$$E(H_{m_{\alpha-1}}) = A \cup B \cup \left(\bigcup_{m_{\alpha-1} \in M_{\alpha-1}} (C_{m_{\alpha-1}} \cup \{[t_{m_\alpha}, (m_{\alpha-1}, t_{m_{\alpha-1}})]\}) \right),$$

où

$$\begin{aligned} A = &\{[(m_{\alpha-1}, t_{m_{\alpha-1}}), (m'_{\alpha-1}, t_{m'_{\alpha-1}})], \\ &[(f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}}), (f_{\alpha-1}(m'_{\alpha-1}), t_{m'_{\alpha-1}})] \mid \\ &m_{\alpha-1}, m'_{\alpha-1} \in M_{\alpha-1}, m_{\alpha-1} \neq m'_{\alpha-1}\}, \\ B = &\{[(m_{\alpha-1}, t_{m_{\alpha-1}}), (f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}})] \mid m_{\alpha-1} \in M_{\alpha-1}\}, \\ C_{m_{\alpha-1}} = &\begin{cases} \{[(m_{\alpha-1}, x), (m_{\alpha-1}, y)] \mid [x, y] \in E(H_{m_{\alpha-1}})\}, & \text{si } m_{\alpha-1} \in M_\alpha, \\ \{[(f_{\alpha-1}(m_{\alpha-1}), x), (f_{\alpha-1}(m_{\alpha-1}), y)] \mid [x, y] \in E(H_{m_{\alpha-1}})\}, \\ \qquad \text{si } m_{\alpha-1} \notin M_\alpha. \end{cases} \end{aligned}$$

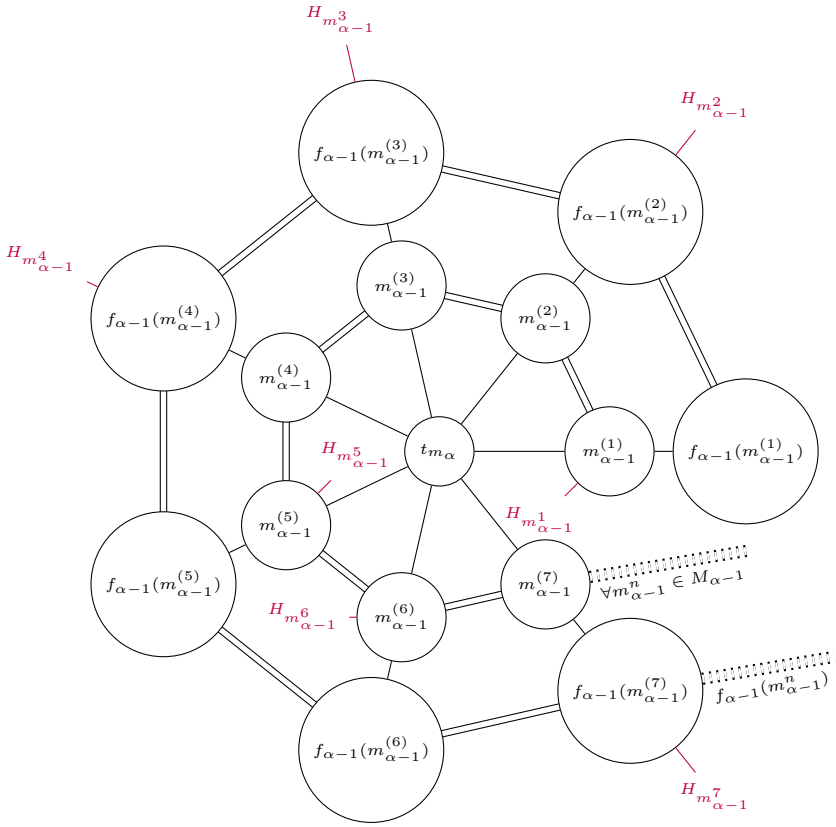


FIGURE 8 – Schéma du graphe de la construction. Cas 1.

— Cas 2 : α est un ordinal limite. Alors pour $m_\alpha \in M_\alpha = \bigcup_{\xi<\alpha} M_\xi$, on pose $\eta = \eta(m_\alpha)$ le plus petit $\xi < \alpha$ tel que $m_\alpha \in M_\xi$ et on définit H_{m_α} par :

$$V(H_{m_\alpha}) = \{t_{m_\alpha}\} \cup V(\sum_{\eta\leq\xi<\alpha} H_{m_\xi}),$$

où $\forall \xi, \eta \leq \xi < \alpha, m_\xi = m_\alpha \in M_\xi$, $t_{m_\alpha} \notin V(\sum_{\eta\leq\xi<\alpha} H_{m_\xi})$ et :

$$E(H_{m_\alpha}) = \{[t_{m_\alpha}, (\xi, t_{m_\xi})] \mid \eta \leq \xi < \alpha\} \cup E(\sum_{\eta\leq\xi<\alpha} H_{m_\xi}).$$

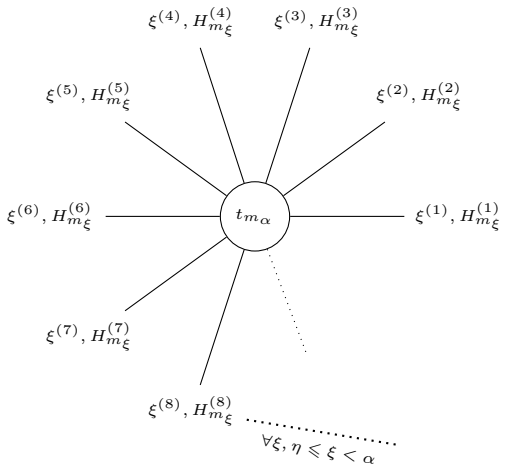


FIGURE 9 – Schéma du graphe de la construction. Cas 2.

Il nous reste à vérifier que cette construction de H_{m_α} vérifie les propriétés 1 à 5 de notre induction. Regardons-les une par une :

1. On souhaite voir que H_{m_α} est connexe.
   - Cas 1 : On va montrer que tout sommet est connecté à t_{m_α}, c'est-à-dire que tous les sommets de $\bigcup_{m_{\alpha-1}\in M_{\alpha-1}} W_{m_{\alpha-1}}$ sont connectés à t_{m_α}.
     Soit $m_{\alpha-1} \in M_{\alpha-1}$. Soit $(x,y) \in W_{m_{\alpha-1}}$, on a affaire à plusieurs cas : Si $m_{\alpha-1} \in m_\alpha$, alors, soit $(x,y) = (f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}})$, qui est connecté à $(m_{\alpha-1}, t_{m_{\alpha-1}})$ grâce à l'ensemble d'arêtes B qui est connecté à $t_{m_{\alpha-1}}$, soit $(x,y) = (m_{\alpha-1}, z)$ avec $z \in V(H_{m_{\alpha-1}})$, or $H_{m_{\alpha-1}}$ est connexe et $m_{\alpha-1} \in M_{\alpha-1}$ donc dans l'ensemble d'arêtes $C_{m_{\alpha-1}}$ il existe une arête de (x,y) vers $(m_{\alpha-1}, t_{m_{\alpha-1}})$, qui est connecté à t_{m_α}. Si $m_{\alpha-1} \notin m_\alpha$, alors soit $(x,y) = (m_{\alpha-1}, t_{m_{\alpha-1}})$ et est donc connecté à t_{m_α}, soit $(x,y) = (f_{\alpha-1}(m_{\alpha-1}), z)$ et donc on a dans $C_{m_{\alpha-1}}$ une arête qui le connecté à $(f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}})$ et donc à t_{m_α}.
   - Cas 2 : Par la définition, les sommets de H_{m_α} sont t_{m_α} ou de la forme (ξ, z) où $z \in V(H_{m_\xi})$. De plus on sait que H_{m_ξ} est connexe donc il existe une arête de (ξ, z) vers (ξ, t_{m_ξ}) et donc vers t_{m_α}.

   Dans tous les cas, tous les sommets sont connectés à t_{m_α} et ainsi H_{m_α} est connexe.
2. Montrons les relations sur les degrés :
   - Cas 1 : Soit $x \in V(H_{m_\alpha})$ étudions son degré en fonction de sa position dans le graphe.
     Si $x = t_{m_\alpha}$ alors ses voisins sont les sommets dans $\{(m_{\alpha-1}, t_{m_{\alpha-1}}) \mid m_{\alpha-1} \in M_{\alpha-1}\}$ donc x de degré $\mathfrak{a}_{\alpha-1}$.
     Soit $m_{\alpha-1} \in M_{\alpha-1}$. Plaçons-nous dans le cas où $m_{\alpha-1} \in m_\alpha$:
     - Si $x = (m_{\alpha-1}, y)$ avec $y \in V(H_{m_{\alpha-1}}) \setminus \{t_{m_{\alpha-1}}\}$ alors ses voisins sont ceux de y dans $H_{m_{\alpha-1}}$ donc de degré au plus $\mathfrak{a}_{\alpha-2}$.
     - Si $x = (m_{\alpha-1}, t_{m_{\alpha-1}})$ alors l'ensemble des sommets voisins de x est :

$$\begin{aligned} &\{t_{m_\alpha}, (f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}})\} \\ \cup &\{(m_{\alpha-1}, z) \mid z \in V(H_{m_{\alpha-1}}) \\ &\qquad \text{tel que } [(m_{\alpha-1}, z), (m_{\alpha-1}, t_{m_{\alpha-1}})] \in E(H_{m_{\alpha-1}})\} \\ \cup &\{(\widehat{m_{\alpha-1}}, t_{\widehat{m_{\alpha-1}}}) \mid \widehat{m_{\alpha-1}} \in M_{\alpha-1}\}, \end{aligned}$$

       ainsi l'ensemble des sommets voisins est composé d'un ensemble de cardinalité $\mathfrak{a}_{\alpha-1}$, un autre qui est l'ensemble des voisins d'un élément d'un $H_{m_{\alpha-1}}$, donc de degré au plus $\mathfrak{a}_{\alpha-2}$ et d'un ensemble à 1 élément, par le Lemme précédent on sait que la cardinalité de cette union est $\mathfrak{a}_{\alpha-1}$.
     - Si $x = (f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}})$ alors l'ensemble de ses voisins est :

$$\{(m_{\alpha-1}, t_{m_{\alpha-1}})\} \cup \{(f_{\alpha-1}(\widehat{m_{\alpha-1}}), t_{\widehat{m_{\alpha-1}}}) \mid \widehat{m_{\alpha-1}} \in M_{\alpha-1}\},$$

       donc x est de degré $\mathfrak{a}_{\alpha-1}$.

Pour le cas $m_{\alpha-1} \notin m_\alpha$, les raisonnements sont les mêmes en inversant le rôle des sommets "$(m_{\alpha-1}, t_{m_{\alpha-1}})$" et "$(f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}})$". Ainsi, on a montré la propriété et on a exhibé des sommets aillant le bon degré.

— Cas 2 : Dans ce cas, on doit montrer qu'il existe un sommet d'ordre α et que celui-ci est de degré plus grand que tous les autres. Par définition on a que le sommet t_{m_α} à pour voisins : $\{(\xi, t_{m\xi}) \mid \eta \leqslant \xi < \alpha\}$ qui est en bijection avec $\{\xi \mid \eta \leqslant \xi < \alpha\} = \bigcup_{\eta \leqslant \xi < \alpha} \xi$ or η contient tous les ordinaux inférieurs à lui par IV.5.10, donc $\bigcup_{\eta \leqslant \xi < \alpha} \xi = \bigcup_{\xi < \alpha} \xi = \alpha$. Donc t_{m_α} est de degré α par la Proposition IV.5.10 (i). De plus par induction tous les autres sommets de H_{m_α} sont inclus dans une copie de H_{m_ξ} pour $\xi < \alpha$, donc sont de degré au pire $\xi + 1 = \xi < \alpha$. On a donc ce qu'on veut.

3. Montrons que $\mathrm{Aut}_{Graph}(H_{m_\alpha}) \cong \{id\}$. Soit $\varphi \in \mathrm{Aut}_{Graph}(H_{m_\alpha})$.

— Cas 1 : Tout d'abord par un Lemme précédent, on a qu'un sommet et son image par φ ont même degré, plus précisément l'ensemble des voisins d'un sommet est en bijection avec l'ensemble des voisins de l'image par φ. Or on a qu'un ensemble de cardinal $\mathfrak{a}_{\alpha-1} = 2^{\mathfrak{a}_{\alpha-2}}$ et un ensemble de cardinal $\mathfrak{a}_{\alpha-2}$ ne sont pas isomorphes. Donc, on peut dire que les ensembles de sommets :

$$A = \bigcup_{\substack{m_{\alpha-1} \in M_{\alpha-1} \\ m_{\alpha-1} \in m_\alpha}} \left(\{m_{\alpha-1}\} \times (V(H_{m_{\alpha-1}}) \setminus \{t_{m_{\alpha-1}}\})\right) \cup \bigcup_{\substack{m_{\alpha-1} \in M_{\alpha-1} \\ m_{\alpha-1} \notin m_\alpha}} \left(\{f_{\alpha-1}(m_{\alpha-1})\} \times (V(H_{m_{\alpha-1}}) \setminus \{t_{m_{\alpha-1}}\})\right),$$

et :

$$B = \{t_{m_\alpha}\} \cup \{(m_{\alpha-1}, t_{m_{\alpha-1}}), (f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}}) \mid m_{\alpha-1} \in M_{\alpha-1}\},$$

sont fixés par φ par les notions de degré. On a de plus par construction que les $(H_{m_{\alpha-1}})_{m_{\alpha-1}}$ restent connexes même si on enlève le sommet $t_{m_{\alpha-1}}$.

Notation : Soit G un graphe et $S \subset V(G)$ un ensemble de sommets de G. On notera G^S le sous-graphe de G tel que :

$$V(G^S) = S,$$
$$E(G^S) = \{[x, y] \in E(H_{m_\alpha}) \mid x, y \in S\}$$

Donc on peut en déduire que le sous-graphe $H^A_{m_\alpha}$, est un graphe qui contient $\mathfrak{a}_{\alpha-1}$ composantes connexes (qui sont toutes des copies du graphe $(H_{m_{\alpha-1}})_{m_{\alpha-1}}$ sans les sommets $t_{m_{\alpha-1}}$) et comme A est fixé par φ on a la relation : $\varphi_{|A} \in \mathrm{Aut}_{Graph}(H^A_{m_\alpha})$. Ainsi les différentes composantes connexes de $H^A_{m_\alpha}$ sont envoyées sur d'autres composantes connexes. Soit K une de ces composantes connexes (on a que c'est un "$H_{m_{\alpha-1}} \setminus t_{m_{\alpha-1}}$"), on prend x_K l'unique sommet de degré $\mathfrak{a}_{\alpha-1}$ connecté à K et donc le graphe $H^{V(K) \cup \{x_K\}}_{m_\alpha}$ est envoyé sur $H^{V(\varphi(K)) \cup \{\varphi(x_K)\}}_{m_\alpha}$, où $\varphi(x_K)$ est un sommet connecté à $\varphi(K)$, donc l'unique de degré $\mathfrak{a}_{\alpha-1}$.

Donc si on considère $C := A \cup \{(m_{\alpha-1}, t_{m_{\alpha-1}}) \mid m_{\alpha-1} \in M_{\alpha-1}, m_{\alpha-1} \in m_\alpha\} \cup \{(f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}}) \mid m_{\alpha-1} \in M_{\alpha-1}, m_{\alpha-1} \notin m_\alpha\}$ alors $H^C_{m_\alpha}$ est un sous-graphe de H_{m_α} contenant lui aussi $\mathfrak{a}_{\alpha-1}$ composantes connexes qui peuvent toutes être mises en correspondance avec un élément de $(H_{m_{\alpha-1}})_{m_{\alpha-1} \in M_{\alpha-1}}$ or, les $(H_{m_{\alpha-1}})_{m_{\alpha-1} \in M_{\alpha-1}}$ ne sont pas isomorphes deux à deux par induction et leur groupe d'automorphisme est réduit à $\{id\}$. On a donc que $\varphi_{|C} = id_C$. Regardons maintenant les sommets dans B. On sait tout d'abord que B est stabilisé par φ. Et on a que tous les sommets qui sont rattachés à des copies de $H_{m_{\alpha-1}}$ sont fixés par φ. Donc le sous-ensemble de B :

$$\begin{aligned}&\{(m_{\alpha-1}, t_{m_{\alpha-1}}) \mid m_{\alpha-1} \in M_{\alpha-1}, m_{\alpha-1} \in m_\alpha\}\\ \cup&\{(f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}}) \mid m_{\alpha-1} \in M_{\alpha-1}, m_{\alpha-1} \notin m_\alpha\},\end{aligned}$$

ne comporte que des sommets fixés par φ. On notera dans la suite : $B^m := \{t_{m_\alpha}\} \cup \{(m_{\alpha-1}, t_{m_{\alpha-1}}) \mid m_{\alpha-1} \in M_{\alpha-1}\}$ et $B^f := \{(f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}}) \mid m_{\alpha-1} \in M_{\alpha-1}\}$. Alors, on voit que les graphes $H^{B^m}_{m_\alpha}$ et $H^{B^f}_{m_\alpha}$ sont des sous-graphes de $H^B_{m_\alpha}$ qui sont complets. On sait qu'un graphe complet et envoyé sur un autre graphe complet par un isomorphisme. Tous les sous-graphes complets de $H^B_{m_\alpha}$ sont soit inclus dans un de nos deux graphes, soit admettent un nombre de sommets bien inférieur à $\mathfrak{a}_{\alpha-1}$. De plus, si (sans perte de généralité) l'image $H^{B^m}_{m_\alpha}$ a pour image un graphe strictement inclus dans $H^{B^f}_{m_\alpha}$ alors les sommets de $H^{B^f}_{m_\alpha}$ qui n'ont pas un antécédent dans $H^{B^m}_{m_\alpha}$ posent un problème, car ils ont une arête en commun avec chaque élément de $\varphi(H^{B^m}_{m_\alpha})$ mais il n'existe pas de tels éléments pour $H^{B^m}_{m_\alpha}$. Donc, on en déduit que $H^{B^m}_{m_\alpha}$ est envoyé sur lui-même ou sur $H^{B^f}_{m_\alpha}$ (pareil pour $H^{B^f}_{m_\alpha}$). De plus, on sait que certains sommets de B sont fixés par φ. On en déduit donc que $H^{B^m}_{m_\alpha} \overset{\varphi}{\mapsto} H^{B^m}_{m_\alpha}$ et $H^{B^f}_{m_\alpha} \overset{\varphi}{\mapsto} H^{B^f}_{m_\alpha}$. On peut également faire la remarque que si on considère une arête $e = [(m_{\alpha-1}, t_{m_{\alpha-1}}), (f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}})]$ alors l'une des deux extrémités est fixée par φ, supposons que c'est $(m_{\alpha-1}, t_{m_{\alpha-1}})$, alors l'arête e est la seule arête connectée à $(m_{\alpha-1}, t_{m_{\alpha-1}})$ qui part de $H^{B^m}_{m_\alpha}$ et qui va dans $H^{B^f}_{m_\alpha}$ donc elle est envoyé sur elle-même. On en déduit donc que tous les sommets de $(B^m \setminus \{t_{m_\alpha}\}) \cup B^f$ sont fixés par φ, et ensuite que t_{m_α} est fixé par φ. Donc $\varphi = id$ et $\mathrm{Aut}_{Graph}(H_{m_\alpha}) \cong \{id\}$.

— Cas 2 : Il est tout d'abord évident que $t_{m_\alpha} \overset{\varphi}{\mapsto} t_{m_\alpha}$. En effet, t_{m_α} est le seul sommet de H_{m_α} qui est de degré α. Considérons donc le sous-graphe stabilisé par φ : $H^{V(H_{m_\alpha}) \setminus \{t_{m_\alpha}\}}_{m_\alpha}$. Ce graphe a une composante connexe par ξ tel que $\eta < \xi < \alpha$, qui est une copie de H_{m_ξ} donc qui n'est isomorphe à aucun autre $H_{m_{\widehat{\xi}}}$ pour $\xi \neq \widehat{\xi}$ et $\eta < \widehat{\xi} < \alpha$, et tel que $\mathrm{Aut}_{Graph}(H_{m_\xi}) \cong \{id\}$. On en déduit facilement que $\varphi_{|V(H_{m_\alpha}) \setminus \{t_{m_\alpha}\}} = id$. Donc $\varphi = id$ et $\mathrm{Aut}_{Graph}(H_{m_\alpha}) \cong \{id\}$.

4. Soit $\widehat{m_\alpha} \in M_\alpha$, montrons que H_{m_α} et $H_{\widehat{m_\alpha}}$ sont isomorphes seulement si $\widehat{m_\alpha} = m_\alpha$ (où $H_{\widehat{m_\alpha}}$ est construit de la même façon que H_{m_α}). Soit $\phi : H_{m_\alpha} \mapsto H_{\widehat{m_\alpha}}$ un isomorphisme de graphes.

Cas 1 : On note :

$$B = \{t_{m_\alpha}\} \cup \{(m_{\alpha-1}, t_{m_{\alpha-1}}), (f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}}) \mid m_{\alpha-1} \in M_{\alpha-1}\}$$
$$\widehat{B} = \{t_{\widehat{m_\alpha}}\} \cup \{(m_{\alpha-1}, t_{m_{\alpha-1}}), (f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}}) \mid m_{\alpha-1} \in M_{\alpha-1}\}$$

ce sont des sous-ensembles de respectivement, $V(H_{m_\alpha})$ et $V(\widehat{m_\alpha})$. Les sommets de ces ensembles sont de degré $\mathfrak{a}_{\alpha-1}$ ce qui n'est pas le cas de tous les sommets de $V(H_{m_\alpha}) \setminus B$ et $V(\widehat{m_\alpha}) \setminus \widehat{B}$. Et en raisonnant de la même façon que dans la partie 3 on a que toutes les copies de $H_{m_{\alpha-1}}$ dans H_{m_α} sont envoyées sur $H_{m_{\alpha-1}}$ dans $H_{\widehat{m_\alpha}}$, il nous reste juste à décider si le sommet représentant $t_{m_{\alpha-1}}$ dans ces copies est $(m_{\alpha-1}, t_{m_{\alpha-1}})$ où $(f_{\alpha-1}(m_{\alpha-1}), t_{m_{\alpha-1}})$. Pour cela on sait que comme dans la partie 3 les sommets des ensemble B^m sont envoyés sur $\widehat{B}^m$ et B^f sur $\widehat{B}^f$ (où on garde là même définition pour $\widehat{B}^m$). Donc, on peut en déduire que pour tout $m_{\alpha-1} \in M_{\alpha-1}$:

$$m_{\alpha-1} \in m_\alpha \Leftrightarrow m_{\alpha-1} \in \widehat{m_\alpha}$$

or $m_\alpha, \widehat{m_\alpha} \in 2^{M_{\alpha-1}} = M_\alpha$, donc pour décrire un élément de M_α il suffit de décrire les éléments de $M_{\alpha-1}$ qui lui sont inclus. On peut donc en déduire que $m_\alpha = \widehat{m_\alpha}$.

Cas 2 : Dans les graphes H_{m_α} et $H_{\widehat{m_\alpha}}$ on a à chaque fois un seul sommet de degré α, donc ϕ envoie l'un sur l'autre : $t_{m_\alpha} \overset{\phi}{\mapsto} t_{\widehat{m_\alpha}}$. De plus, si on considère les graphes privés de ces sommets $H_{m_\alpha}^{V(H_{m_\alpha}) \setminus \{t_{m_\alpha}\}}$ et $H_{\widehat{m_\alpha}}^{V(H_{\widehat{m_\alpha}}) \setminus \{t_{\widehat{m_\alpha}}\}}$ alors ils contiennent tous deux α composantes connexes et ces composantes connexes sont envoyées par ϕ sur d'autres. Prenons donc H_{m_ξ} une copie d'un des sous-graphes de $H_{m_\alpha}^{V(H_{m_\alpha}) \setminus \{t_{m_\alpha}\}}$, ainsi on a que $m_\xi = m_\alpha$ vu dans M_ξ, il est envoyé sur H_{m_ζ} une copie d'un des sous-graphes de $H_{\widehat{m_\alpha}}^{V(H_{\widehat{m_\alpha}}) \setminus \{t_{\widehat{m_\alpha}}\}}$ avec $m_\zeta = \widehat{m_\alpha}$ vu dans M_ζ. Mais par induction, on a que si $m_\zeta \neq m_\xi$ alors les graphes H_{m_ζ} et H_{m_ξ} ne sont pas isomorphes. Donc, on en déduit que $m_\alpha = m_\xi = m_\zeta = m_{\widehat{\alpha}}$.

5. Soient $\eta < \alpha$, $m_\eta \in M_\eta$, montrons que H_{m_η} et H_{m_α} ne sont pas isomorphes.
   - Cas 1 : On sait par le point 2 que tous les sommets de H_{m_η} sont de degré au plus $\mathfrak{a}_{\eta-1}$, alors que dans H_{m_α} il existe un sommet de degré $\mathfrak{a}_{\alpha-1}$. Et comme $\eta < \alpha$, alors $\mathfrak{a}_{\eta-1} < \mathfrak{a}_{\alpha-1}$, ainsi H_{m_η} et H_{m_α} ne sont pas isomorphes.
   - Cas 2 : De là même façon, dans ce cas, on a que si, $\eta \neq \xi$ alors on peut les comparer, ainsi on peut supposer sans perte de généralité que $\eta < \xi$, par le Corollaire IV.5.12. Ainsi dans H_{m_ξ} il y a un sommet de degré ξ, alors que dans H_{m_η}, tous les sommets sont de degrés strictement inférieurs (pour l'ordre des ordinaux) à ξ.

On va donc maintenant construire les graphes qui nous intéressent dans l'énoncé. Soit $\alpha \in \mathcal{A}$. Si α n'est pas un ordinal limite alors on prend $m_\alpha \in M_\alpha$ et on note :

$$x_\alpha := t_{m_\alpha}$$
$$H_\alpha := H_{m_\alpha}$$

et si α est un ordinal limite on prend $x_\alpha \notin V(\sum_{m_\alpha \in M_\alpha} H_{m_\alpha})$ et on définit H_α de la façon suivante :

$$V(H_\alpha) := \{x_\alpha\} \cup V(\sum_{m_\alpha \in M_\alpha} H_{m_\alpha}),$$
$$E(H_\alpha) := \{[x_\alpha, (m_\alpha, t_{m_\alpha})] \mid m_\alpha \in M_\alpha\} \cup E(\sum_{m_\alpha \in M_\alpha} H_{m_\alpha}).$$

Dans tous les cas H_α est connexe. Si α n'est pas un ordinal limite, on a déjà vu que $\mathrm{Aut}_{Graph}(H_\alpha) \cong \{id\}$, si c'est un ordinal limite, on peut répéter la même étude que pour le point 3 de l'induction et obtenir également $\mathrm{Aut}_{Graph}(H_\alpha) \cong \{id\}$. De plus, encore une fois grâce à l'induction, si $\alpha, \beta \in \mathcal{A}$ et $\alpha \neq \beta$ alors H_α et H_β ne sont pas isomorphes.

On peut également faire la remarque que tous les sommets de degré 2 dans ces graphes proviennent de H_{m_0} où $m_0 \in \mathbb{N}$ et donc que tous les voisins sont de degré inférieur ou égal à $\aleph_0$. □

Preuve (Théorème). Soit $(G, *_G)$ un groupe. Prenons A un ensemble contenant des ordinaux tel que le cardinal de A est le cardinal de G. Ainsi $G = \{h_\alpha \mid \alpha \in A\}$. On prend pour tout $\alpha \in A$, le graphe H_α et le sommet x_α construit dans le Lemme. Pour tout $(\alpha, g) \in A \times G$, on note H_α^g le graphe isomorphe à H_α tel que :

$$V(H_\alpha^g) = \{(x, g) \mid x \in V(H_\alpha)\}$$
$$E(H_\alpha^g) = \{[(x, g), (y, g)] \mid [x, y] \in E(H_\alpha)\}$$

Et on notera $x_\alpha^g = (x_\alpha, g)$. Finalement, on construit le graphe H suivant :

$$\begin{aligned} V(H) =& G \cup \mathcal{A} \times G \cup V(\sum_{\alpha \in \mathcal{A}, g \in G} H_\alpha^g), \\ E(H) =& \{[g, (\alpha, g)], [(\alpha, g), x_\alpha^g], [x_\alpha^g, g *_G h_\alpha] \mid \alpha \in \mathcal{A}, g \in G\} \\ & \cup E(\sum_{\alpha \in \mathcal{A}, g \in G} H_\alpha^g) \end{aligned}$$

On a clairement que H est connexe. Il nous reste à montrer que $\mathrm{Aut}_{Graph}(H) \cong G$. Pour cela, faisons tout d'abord la remarque que la construction de H est simplement le graphe de Cayley $\mathcal{C}(G)$ coloré pour lequel on a remplacé chaque arête orientée de g à $\widehat{g}$ et coloré g_α (donc $g^{-1}\widehat{g} = h_\alpha$) par le graphe $K_\alpha^g = (V_\alpha^g, E_\alpha^g)$ définit par :

$$V_\alpha^g = \{(\alpha, g)\} \cup V(H_\alpha^g),$$
$$E_\alpha^g = \{[(\alpha, g), x_\alpha^g]\} \cup E(H_\alpha^g),$$

connecté au sommet g par l'arête (α, g) et connecté à $\widehat{g}$ par x_α^g. On peut le représenter comme ci dessus :

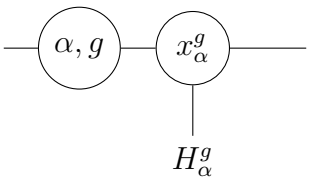


FIGURE 10 – Le graphe K_α^g

On remarque que les graphes $(K_\alpha^g)_{\alpha\in\mathcal{A},g\in G}$ vérifient bien les propriétés nécessaires à l'application de la démonstration du théorème de Frucht. En effet, ce sont des graphes connexes, si $\alpha \neq \beta$ dans $\mathcal{A}$ alors par le Lemme précédent K_α^g et K_β^g ne sont pas isomorphes et $\mathrm{Aut}_{Graph}(K_\alpha^g) \cong \{id\}$ (en effet, on a déjà vu que c'était vrai pour H_α^g et le sommet (α, g) est forcément stabilisé, car c'est le seul de degré 2 qui a un voisin d'ordre supérieur à $\aleph_0$). Finalement, comme dans les théorèmes précédents, en reprenant la démonstration du théorème de Frucht on a que $\mathrm{Aut}_{Graph}(H) \cong G$.□

VI Corps

VI.1 Les extensions de $\mathbb{Q}$ en tant que catégorie

Definition VI.1.1 Un *anneau* est un triplet $(A, +, \times)$, où A est un ensemble et $+$ et $\times$ des lois de composition interne telles que :

— $(A, +)$ est un groupe abélien.

— $\times$ est associative, distributive par rapport à $+$ et elle possède un élément neutre 1_A.

Comme pour les groupes, on notera A l'anneau au lieu de $(A, +, \times)$ et si $\times$ est commutative et appellera A un anneau commutatif.

Definition VI.1.2 Un *corps* est un triplet $(K, +, \times)$, où K est un ensemble, et on vérifie :

— le triplet $(K, +, \times)$ est un anneau commutatif,

— tout élément non nul de K possède un inverse par rapport à la loi $\times$,

— $0_K \neq 1_K$, où 0_K et 1_K désignent le neutre de K pour respectivement, $+$ et $\times$.

Le but de cette section est de voir les extensions de $\mathbb{Q}$ comme une catégorie.

Definition VI.1.3 Soit K un corps. Une *extensions de corps* de K est un couple (L, j) où L est un corps et $j : K \to L$ est un morphisme de corps (et donc injectif). On la note L/K.

Remarque: Il est toujours possible de voir une extension de corps comme un "sur"-corps du corps de base. Pour faciliter les choses, nous confondrons dans la suite ces deux notions et nous verrons une extension L/K comme une inclusion $K \subset L$.

Definition VI.1.4 Soient L/K,M/K deux extensions et une application $f : L \to M$. On dit que f est un *morphisme d'extensions* si :

— f est un morphisme de corps, c'est-à-dire un *morphisme d'anneaux* entre deux corps, c'est-à-dire :

$$\forall a, b \in L, f(a + b) = f(a) + f(b) \text{ et } f(ab) = f(a)f(b) \text{ et } f(1_A) = f(1_B).$$

— f stabilise K, c'est-à-dire : $f_{|_K} = id_K$.

Avec ces deux définitions, on voit que si l'on se fixe K un corps de base, alors la classe de toutes les extensions de K est une catégorie, muni des morphismes d'extensions. En particulier, les extensions de $\mathbb{Q}$ forment une catégorie et donc nous pouvons nous poser la question de la réalisabilité de groupe sur cette catégorie.

VI.2 Notions de théorie de Galois

L'objectif principal de cette section est de montrer l'énoncé suivant. Pour cela nous allons réintroduire des notions élémentaires sur les corps et de théorie de Galois, cependant pour plus détails l'auteur pourra se référer à la source [1].

Théorème VI.2.1 (van der Waerden) *Soit $n \in \mathbb{N}$. Il existe $P \in \mathbb{Q}[X]_{<p}$ tel que son groupe de Galois est isomorphe à $\mathfrak{S}_n$.*

Pour cela, on commence par quelque généralités.

Definition VI.2.2 (Corps de décomposition) Soit K un corps, soit $P \in K[X]$ un polynôme et, soit L/K une extension de K. On dit que L est un *corps de décomposition* de P sur K si :

— P est scindé dans $L[X]$.

— L est engendré par les racines de P (qui existent dans L car P y est scindé).

Definitions VI.2.3 (Groupe de Galois) Soit K un corps.

i) Soit $L/K, L'/K$ deux extensions. On définit un K-morphisme (*resp.* K-isomorphisme) d'extension de L/K sur L'/K un morphisme (*resp.* isomorphisme) de corps $\alpha : L \to L'$ tel que $\alpha_{|_K} = id_K$.

ii) Soit L/K une extension. On définit la *groupe de Galois* de L/K comme étant le groupe de K-automorphismes (*i.e.* les K-isomorphisme de L/K dans lui-même) de l'extension L/K. On le note $\mathrm{Gal}(L/K)$

iii) Soit $P \in K[X]$. Le *groupe de Galois de P* est le groupe de Galois de son corps des racines. On le note $\mathrm{Gal}_K(P)$.

Remarque: On confondra dans la suite la notion de K-automorphisme de L et celle d'automorphisme de L/K.

Definitions VI.2.4 (Groupe de permutation) Soit X un ensemble et $n \in \mathbb{N}$.

i) On définit *le groupe des permutations* de X comme l'ensemble des bijections de X dans X muni de la composition. On le note $\mathfrak{S}(X)$. De façon générale, on notera $\mathfrak{S}_n = \mathfrak{S}(\llbracket 1, n \rrbracket)$.

ii) On définit *un groupe de permutations* sur X comme un sous-groupe de $\mathfrak{S}(X)$.

iii) Soit $\tau = (i_1 \ ... \ i_m) \in \mathfrak{S}_n$ un m-cycle, on appelle $\{i_1, ..., i_m\}$ son *support*.

iv) Soit $\sigma = \tau_1 \circ ... \circ \tau_r \in \mathfrak{S}_n$ où chaque τ_i est un m_i-cycle et ils ont deux à deux supports disjoints. On dit dans ce cas que σ est de *type* $[m_1 \ ... \ m_r]$.

Definitions VI.2.5 Soit K un corps.

i) Soit $P \in K[X], P \neq 0$ un polynôme de degré n. Si L est un corps de décomposition de P sur K on dit que P est *séparable* sur K si P possède n racines distinctes dans L.

ii) Si $|K| = q$. Soit L/K une extension finie de K. L'application :

$$Fr_q : \begin{array}{ccc} K & \to & K \\ x & \mapsto & x^q \end{array},$$

est appelée automorphisme de Frobenius de L/K.

Definition VI.2.6 Soit G un groupe de permutations sur X et G' un groupe de permutations sur X'. S'il existe $f : X \to X'$ une application bijective et $\lambda : G \to G'$ un isomorphisme tel que pour tout $g \in G$ et tout $x \in X$, $f(g(x)) = \lambda(g)(f(x))$, alors G et G' sont dis *isomorphe en tant que groupes de permutations.*

Après ces nombreuses définitions, il nous faut quelques énoncés pour arriver au théorème. On peut tout d'abord rappeler que si $P \in K[X]$ est un polynôme de degré $n \geqslant 1$, alors on peut définir une action de $\mathrm{Gal}_K(P)$ sur l'ensemble des racines X_P de P, définie par :

$$\begin{array}{ccccc} \mathrm{Gal}_K(P) & \times & X_P & \to & X_P \\ (\sigma & , & \alpha) & \mapsto & \sigma(\alpha), \end{array}$$

et que cette action est fidèle, i.e. que le morphisme associé $\left\{ \begin{array}{ccc} \mathrm{Gal}_K(P) & \to & \mathfrak{S}(X_P) \\ \sigma & \mapsto & \sigma_{|X_P} \end{array} \right.$ est injectif.

Definition VI.2.7 Soit L/K une extension de corps. On dit que L/K est une extension galoisienne si :

- L/K est séparable : Pour tout $a \in L$, le polynôme minimal de a est à racines simples dans une clôture algébrique $\overline{K}$ de K.
- L/K est normale : L est le corps de décomposition d'un polynôme de $K[X]$.

Pour le prochain énoncé nous auront besoin de rappeler un théorème élémentaire de théorie des corps, nous n'en donneront pas de démonstration ici, mais le lecteur pourra en trouver une dans la source [1].

Théorème VI.2.8 (de prolongement des isomorphismes) *Soit K un corps et soit L/K une extension et soit $\alpha \in L$ un élément algébrique sur K. Soit M un corps quelconque et soit $\iota : K \to M$ un morphisme d'anneaux. Alors l'ensemble des morphismes d'anneaux $\sigma : K(\alpha) \to M$ prolongeant ι est en bijection avec l'ensemble des racines de $\iota(\mu_{\alpha,K})$ dans M (où $\mu_{\alpha,K}$ désigne le polynôme minimal de α sur K).*

Lemme VI.2.9 *Soit K un corps et $P \in K[X]$ séparable de degré n. On prend L un corps de décomposition de P sur K et on note S l'ensemble des racines de P dans L. Alors $G = \mathrm{Gal}(L/K)$ agit transitivement sur S si et seulement si P est irréductible sur $K[X]$.*

Preuve. On peut rapidement vérifier que L/K est une extension galoisienne en tant que corps de rupture d'un polynôme (donc normal) séparable (donc engendré par racines de P qui sont des éléments séparables), de plus P étant irréductible on peut appliquer le Théorème VI.2.8 et on obtient donc que $G = \mathrm{Gal}(L/K) = \mathfrak{X}(L/K)$ agit sur S transitivement.

Inversement, supposons que $P = QR$ où $Q, R \in K[X]$ sont de degré dans $[\![1, n-1]\!]$. Si on note T l'ensemble des racines de Q alors on a également que G agit sur $T \neq S$ et donc forcément il existe plus d'une orbite donc l'action n'est pas transitive. □

Corrolaire VI.2.10 *Soit K un corps et $P = P_1...P_r \in K[X]$ séparable, où $f_i \in F[X]$ sont des polynômes irréductibles. Soient L est un corps de décomposition de P, $G = \mathrm{Gal}(L/K)$, S l'ensemble des racines de P dans L et pour tout $i \in [\![1, r]\!]$,S_i l'ensemble des racines de P_i dans L. Alors $S = \sqcup_{i\in[\![1,r]\!]} S_i$ est une union disjointe et chaque S_i est une orbite sous l'action de G.*

Preuve. Immédiat avec le Lemme VI.2.9. □

Lemme VI.2.11 *Soient K un corps fini et L/K une extension finie de K de degré n. Alors L/K est une extension galoisienne et $\mathrm{Gal}(L/K)$ est un groupe cyclique d'ordre n engendré par l'automorphisme Fr_p de Frobenius.*

Preuve. Notons $|K| = q$ et $[L : K] = n$ (cela signifie en particulier que $L \cong \mathbb{F}_{q^n}$). Dans ce cas $|L^\times| = |L^*| = q^n - 1$, donc pour tout $x \in L^*, x^{q^n-1} = 1$ et ainsi pour tout $x \in L, x^{q^n} = x$ et donc $Fr_p^n = id_K$.

Ainsi, on a que l'ordre de Fr_p divise n, montrons que c'est n. Soit $m \in \mathbb{N}, 1 \leqslant m < n$, si on suppose par l'absurde que $Fr_p^m = id_K$ alors pour tout $x \in L, Fr_p^m(x) = x^{q^m} = x$ donc le polynôme $X^{q^m} - X$ a $|L| = q^n > q^m$ racines, ce qui est impossible, car ce polynôme est de degré q^m. Ainsi Fr_p est d'ordre n de plus $\langle Fr_p\rangle$ est un sous-groupe de $\mathrm{Gal}(L/K)$, donc on a $n \leqslant |\mathrm{Gal}(l/K)| \leqslant [L : K] = n$. Ainsi L/K est galoisienne est $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$. □

Lemme VI.2.12 *Soient K un corps fini et $P \in K[X]$ irréductible de degré n. Soit L un corps de décomposition de P sur K. Alors $\mathrm{Gal}(L/K)$ est un groupe cyclique engendré par le morphisme Fr_p de Frobenius.*

Preuve. Soit α une racine de P dans L. On applique le Lemme VI.2.11 à $K(\alpha)/K$ une extension finie de K et on obtient quelle est galoisienne donc normale. De plus, on sait que tout polynôme irréductible admettant une racine dans une extension normale est scindé (par définition). Donc P étant irréductible, P est scindé dans $K(\alpha)$ et on en déduit que $K(\alpha)$ est un corps de décomposition de P, et comme $K(\alpha) \subset L$, on a $L = K(\alpha)$.

Toujours en appliquant le Lemme VI.2.11 on obtient que :
$\mathrm{Gal}(L/K) = \mathrm{Gal}(K(\alpha)/K)$ est un groupe cyclique d'ordre n engendré par σ le morphisme de Frobenius. □

Corrolaire VI.2.13 *Soient K un corps fini et $P \in K[X]$ irréductible de degré n. Soient L un corps de décomposition de P sur K, $G = \mathrm{Gal}(L/K)$ et S l'ensemble des racines de P. Si on regarde G comme un groupe de permutations sur S alors Fr_p est un n-cycle.*

Preuve. Une permutation d'ordre n sur un ensemble à n éléments est un n-cycle, le reste suit du Lemme VI.2.12. □

Finalement l'énoncé résumant tout ce que l'on vient de faire sur les corps finis et les cycles :

Lemme VI.2.14 *Soient K un corps fini et $P \in K[X]$ séparable. On suppose que $P = P_1...P_r$ où les P_i sont des polynômes irréductibles différents de $F[X]$, on note ensuite pour tout $i \in [\![1, r]\!]$, $m_i = degP_i$. Soient L un corps de décomposition de P sur K, $G = \mathrm{Gal}(L/K)$ et S l'ensemble des racines de P. Si on regarde G comme un groupe de permutations sur S alors Fr_p est une permutation de type $[m_1 \dots m_r]$.*

Preuve. En appliquant les énoncés : VI.2.10, VI.2.11 et VI.2.13, le résultat suit immédiatement. □

Lemme VI.2.15 *Le groupe $\mathfrak{S}_n$ est engendré par l'ensemble des transpositions de la forme $(k\ n)$ pour $k \in [\![1, n-1]\!]$.*

Preuve. On sait tout d'abord le fait que tout élément $\sigma \in \mathfrak{S}_n$ peut se décomposer en produit de transpositions, ainsi l'ensemble des transpositions engendre $\mathfrak{S}_n$. Soit $(a\ b) \in \mathfrak{S}_n$ une transposition, si a ou b est égal à n alors $(a\ b) \in \{(k\ n) \mid k \in [\![1, n]\!]\} \subset \langle (k\ n) \mid k \in [\![1, n]\!] \rangle$. Si maintenant $a \neq n$ et $b \neq n$ alors $(a\ b) = (a\ n)(b\ n)(a\ n) \in \langle (k\ n) \mid k \in [\![1, n]\!] \rangle$. Donc $\langle (k\ n) \mid k \in [\![1, n]\!] \rangle = \mathfrak{S}_n$. □

Lemme VI.2.16 *Soit G un groupe de permutations d'un ensemble fini X, $n = |G|$, supposons que G agit transitivement sur X et que G contient une transposition et un $(n-1)$-cycle. Alors G est $\mathfrak{S}(X)$.*

Preuve. G est un sous-groupe de $\mathfrak{S}_n$. Comme X est fini, on peut supposer sans perte de généralité que $X = \{1, ..., n\}$. On note $\tau = (1\ ...\ n-1), (i\ j) \in G$ les éléments de l'énoncé. Comme $G \circlearrowleft X$ est transitive, il existe $\sigma \in G$ tel que $\sigma(j) = n$. On note $k = \sigma(i)$, donc $k \neq n$ et on a $\sigma(i\ j)\sigma^{-1} = (k\ n) \in G$. On vérifie ensuite que pour tout $m \in [\![1, n-1]\!]$:

$$(n\ m) = \begin{cases} \tau^{m-k}(k\ n)(\tau^{m-k})^{-1}, \text{ si } m \geqslant k, \\ \tau^{n+m-k+}(k\ n)(\tau^{n+m-k})^{-1}, \text{ si } m < k, \end{cases}$$

et donc par le Lemme VI.2.15 on a que $G = \mathfrak{S}_n$. □

Lemme VI.2.17 *Soient K un corps fini et $n \in \mathbb{N}^*$. Alors, il existe un polynôme de degré n irréductible dans $K[X]$.*

Preuve. Notons $|K| = q$ et prenons L un corps de décomposition de $P = X^{q^n} - X \in K[X]$. On considère S l'ensemble des racines de P dans L. C'est un sous-corps de L (facile à voir avec le morphisme de Frobenius sur K) contenant K (car les éléments de K sont racines de $X^q - X$). De plus, comme L est engendré par les racines de P, donc $S = L$. $P' = q^n X^{q^n-1} - 1 \neq 0$ donc P est séparable et comme il est de degré q^n on a $|S| = q^n$ et donc $[L : K] = n$. De plus L étant un corps fini on a que L^* est cyclique, on prend α un générateur et on a $L = K(\alpha)$ (pour tout $x \in L^*$, $x = \alpha^k$). Finalement, $\mu_{\alpha,K} \in K[X]$ est un polynôme irréductible de degré $[K(\alpha) : K] = [L : K] = n$. □

Lemme VI.2.18 *Soient $P \in \mathbb{Z}[X]$ un polynôme unitaire et p un nombre premier. Supposons que $P \mod p$ soit séparable dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors P est séparable dans $\mathbb{Q}$.*

Preuve. Raisonnons par contraposée et supposons que P n'est pas séparable dans $\mathbb{Q}$. Dans ce comme $\mathbb{Q}$ est parfait on sait que P n'est pas irréductible donc on peut prendre $Q \in \mathbb{Z}[X]$ un facteur irréductible unitaire de P tel que Q^2 divise aussi P. Alors on a que $\deg Q > 0$ et comme Q est unitaire, $\deg(Q \mod p) = \deg Q$. Et comme $Q^2 \mod p$ divise $P \mod p$ on a que $P \mod p$ n'est pas non plus séparable. □

L'énoncé suivant n'est pas évident, mais il contient en lui le nœud de la preuve.

Théorème VI.2.19 *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire. Soit p premier et, soit $\bar{P} \in \mathbb{F}_p[X]$ sa réduction modulo p. On suppose que $\bar{P}$ est séparable. Alors, il existe un morphisme de groupes injectif*

$$\mathrm{Gal}_{\mathbb{F}_p}(\bar{P}) \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(P).$$

De plus, si $d_1, ..., d_r$ sont les degrés des facteurs irréductibles unitaires de $\bar{P}$, alors $\mathrm{Gal}_{\mathbb{Q}}(P)$ contient une permutation de type $[d_1...d_r]$.

Preuve. Admis ici, le lecteur pourra se référer à la source [1]. □

On arrive enfin à la démonstration du théorème.

Preuve (Théorème VI.2.1). Soit $n \in \mathbb{N}^*$. Soit P_1 un polynôme irréductible unitaire de degré n dans $\mathbb{Z}/2\mathbb{Z}[X]$ (par le Lemme VI.2.17).

Soient Q_0 un polynôme unitaire de degré 1 dans $\mathbb{Z}/3\mathbb{Z}[X]$, $Q_1 \neq Q_0$ un polynôme unitaire irréductible de degré $n-1$ dans $\mathbb{Z}/3\mathbb{Z}[X]$. On pose $P_2 = Q_0Q_1$. Alors P_2 est séparable, car Q_1 irréductible et Q_0 de degré 1.

Soit R_0 un polynôme unitaire irréductible de degré 2 dans $\mathbb{Z}/5\mathbb{Z}[X]$. Si $n-2$ est impair, soit R_1 un polynôme unitaire irréductible de degré $n-2$ dans $\mathbb{Z}/5\mathbb{Z}[X]$. On pose $P_3 = R_0R_1$.Supposons par l'absurde que P_3 n'est pas séparable, R_0 et R_1 l'étant, on obtient qu'il existe $\alpha \in \overline{\mathbb{Z}/5\mathbb{Z}}$ une racine de R_0 et, R_1 mais donc comme R_0 et R_1 sont irréductibles on a $\mu_{\alpha,\mathbb{Z}/5\mathbb{Z}} = R_0 = R_1$ mais leurs degrés étant différents, on a $R_0 \neq R_1$ donc on a une contradiction et P_3 est séparable. Si $n-2$ est pair, il existe un $a \in \mathbb{N}$ impair tel que $n-1 = 1+a$, soit $R_1 \neq R_2$ deux polynômes irréductibles unitaires de degré 1 et a respectivement dans $\mathbb{Z}/5\mathbb{Z}[X]$. On pose $P_3 = R_0R_1R_2$ qui est séparable (de la même façon que pour le cas $n-2$ impair).

On pose $P = -15P_1 + 10P_2 + 6P_3$, comme les P_i le sont, P est unitaire de degré n. Alors, on a que :

$$\begin{aligned} P &\equiv P_1 \mod 2 \\ P &\equiv P_2 \mod 3 \\ P &\equiv P_3 \mod 5 \end{aligned}$$

P_1 étant irréductible sur $\mathbb{Z}/2\mathbb{Z}[X]$, P l'est sur $\mathbb{Q}[X]$. On prend L un corps de rupture de P sur $\mathbb{Q}$, $G = \mathrm{Gal}(L/\mathbb{Q})$ et M l'ensemble des racines de P dans L. On regarde G comme un groupe de permutations sur M. Par le Lemme VI.2.9 on sait que, comme P est irréductible, G agit transitivement sur M.

Comme $P \equiv P_2 \mod 3$ est irréductible de degré $n-1$, G contient un $(n-1)$-cycle par le Théorème VI.2.19. De la même manière $P \equiv P_3 \mod 5$, G contient une permutation τ de type $[2\ a]$ ou de type $[2\ 1\ a]$ où a est un entier impair. Alors τ^a est une transposition qui est dans G. Donc G est le groupe symétrique sur M par le Lemme VI.2.16. □

VI.3 Réalisabilité sur la catégorie des extensions de $\mathbb{Q}$

Dans cette section, nous allons nous intéresser à la réalisabilité de groupe de la catégorie des extensions finies de $\mathbb{Q}$. Cette question a été introduite par Emmy Noether dans le contexte plus général suivant :

Question : Pour tout groupe fini G existe-t-il un corps K_G tel que $K_G/\mathbb{Q}$ est finie, algébrique et normale, et tel que $\mathrm{Aut}_{extension}(K_G) \cong G$?

Nous montrerons donc dans cette section un énoncé plus faible qui ne prend pas en compte la notion d'extension normale :

Théorème VI.3.1 *Pour tout groupe fini G, il existe une extension finie algébrique K_G de $\mathbb{Q}$ tel que $\mathrm{Aut}_{extension}(K_G) \cong G$.*

Pour arriver à ce résultat, nous avons besoin de deux Lemmes préliminaires, mais avant ça commençons par une proposition plus générale.

Proposition VI.3.2 *Soient p un nombre premier et K un corps. Soit $a \in K$. Si $X^p - a \in K[X]$ n'a pas de racine dans K, alors $X^p - a$ est irréductible sur L.*

Preuve. Supposons par contraposée que $X^p - a = PQ$ avec $P, Q \in K[X]$ et $\deg(P)$, $\deg(Q) \in [\![1, p-1]\!]$. Alors dans $\overline{K}$ on a que $P = \prod_{i=1}^{m}(X - \alpha_i)$, donc $P(0) = \prod_{i=1}^{m}(-\alpha_i)$ et les α_i sont des racines de a d'ordre divisant p (soit 1, soit p, car p premier). Ainsi $P(0)^p = (-1)^{mp}\prod_{i=1}^{m}\alpha_i^p = (-1)^{mp}a^m$ donc $((-1)^m P(0))^p = a^m$ et donc on pose $b = (-1)^m P(0)$. De plus $m \in [\![1, p-1]\!]$ donc $p \wedge m = 1$ car p est premier. Ainsi par le théorème de Bézout, on a qu'il existe $u, v \in \mathbb{Z}$, tels que $pu + mv = 1$, ce qui donne : $b^{pv} = a^{mv} = a^{1-pu}$. Finalement $a = \left(\frac{b^v}{a^u}\right)^p$, donc $\frac{b^v}{a^u} \in K$ est racine de $X^p - a$. Mais on a supposé que $X^p - a$ n'a pas de racine dans K, ce qui est absurde, donc on a que $X^p - a$ est irréductible sur L. □

Lemme VI.3.3 *Soient p un nombre premier et K un corps. Supposons qu'il existe $a \in K$ tel que $X^p - a \in K[X]$ n'admet pas de racines dans K. Si pour un $b \in K$ on a $\sqrt[p]{b} = K(\sqrt[p]{a})$, alors il existe $c \in K, k \in \mathbb{N}, k < p$ tel que $\sqrt[p]{b} = c(\sqrt[p]{a})^k$.*

Preuve (Lemme VI.3.3). Soit ε une racine primitive p-ème de l'unité et, soit $L = K(\varepsilon)$. Comme p est premier et que $X^p - a$ n'a pas de racines dans K, il est irréductible dans K par la Proposition VI.3.2. L'extension L/K est galoisienne. En effet, cette extension est déjà séparable, car elle est engendrée par ε qui est racine de $X^p - 1$, ainsi $\mu_{\varepsilon,K} | X^p - 1$ et donc comme $X^p - 1$ est séparable (en caractéristique différente de p), $\mu_{\varepsilon,K}$ l'est aussi et donc ε aussi. De plus elle est normale : elle contient ε racine primitive p-ème de l'unité, donc l'ensemble $\{\varepsilon^k \mid k = 0, ..., p-1\}$ contient p éléments différents qui sont tous des racines de $X^p - 1$, ce sont donc l'ensemble de toutes ces racines et on voit ensuite que L est un corps de décomposition de $X^p - 1$ sur K, donc en particulier une extension normale. L'extension L/K est également de degré strictement plus petit que p car $[L : K] = deg_K(\varepsilon) = deg(\mu_{\varepsilon,K}) \leqslant deg(X^{p-1} + ... + x + 1) = p - 1$. On en déduit que $X^p - a$ n'a pas de racines non plus sur L, en effet supposons qu'il existe $x \in L$ tel que $x^p - a = 0$ alors comme $X^p - a \in K[X]$ est irréductible, on en déduit que $\mu_{x,K} = X^p - a$ donc $[K(x) : K] = p | [L : K] < p$, ce

qui est absurde, donc $X^p - a$ n'a pas de racines dans L et par la Proposition VI.3.2, $X^p - a$ est irréductible sur L.

Par l'énoncé, on sait que l'on a $\sqrt[p]{b} = P(\sqrt[p]{a})$ où $P \in K[X]_{<p}$ (où P peut-être pris de degré strictement plus petit que p, car $deg_K(\sqrt[p]{a}) = p$). De plus l'extension $L(\sqrt[p]{a})/K$ est galoisienne et donc on peut montrer que l'on a $P(\varepsilon.\sqrt[p]{a}) = (\varepsilon)^k.\sqrt[p]{b}$ pour $0 \leqslant k < p$. En effet, de $\sqrt[p]{b} = P(\sqrt[p]{a})$ on déduit que $P(\sqrt[p]{a})^p - b = 0$, donc $\sqrt[p]{a}$ est une racine de $P(X)^p - b \in K[X]$ donc $\mu_{\sqrt[p]{a},K} = X^p - a | P(X)^p - b$, en particulier toute racine de $X^p - a$ est une racine de $P(X)^p - b$ ainsi $P(\varepsilon.\sqrt[p]{a})^p - b = 0$. Or les racines de $X^p - b$ sont les $\varepsilon^k.\sqrt[p]{b}$ pour $0 \leqslant k < p$, donc on a bien $P(\varepsilon.\sqrt[p]{a}) = (\varepsilon)^{k_0}.\sqrt[p]{b}$ pour $0 \leqslant k_0 < p$. On en déduit que $\sqrt[p]{a}$ est une racine de $Q(X) = P(\varepsilon.X) - (\varepsilon)^{k_0}.P(X) \in L[X]$ qui est un polynôme de degré strictement plus petit que p. Or $X^p - a$ étant irréductible on a $X^p - a = \mu_{\sqrt[p]{a},K} | Q$ et ainsi $Q \equiv 0$. On note maintenant $P = \sum_{k=0}^{p-1} a_k X^k$ et on a : $\sum_{k=0}^{p-1} a_k(\varepsilon.X)^k = (\varepsilon)^{k_0}.\sum_{k=0}^{p-1} a_k X^k$ et en regardant chaque degré on a : $\forall k \in [\![0, p-1]\!], a_k.\varepsilon^k = \varepsilon^{k_0}.a_k$, on en déduit que $\forall k \in [\![0, p-1]\!], a_k.\varepsilon^{k_0-k} = a_k$ et donc $\forall k \neq k_0, a_k = 0$, ce qui nous donne $P = a_{k_0}X^{k_0}$ et on en déduit facilement le résultat.

On introduit les définitions suivantes.

Definitions VI.3.4 — Un *corps de nombres algébriques* est une extension finie $L/\mathbb{Q}$ de $\mathbb{Q}$.

— Soit L un corps de nombres algébriques. Soit $a \in L$. On dit que a est un *entier algébrique* de L s'il existe $P \in \mathbb{Z}[X]$ tel que $P(a) = 0$.

— Soit L un corps de nombres algébriques. L'*anneau des entiers* de L est l'anneau contenant tous les entiers algébriques de L.

Remarques:

1. Soit L un corps de nombres algébriques. En particulier L contient $\mathbb{Q}$ et $\mathbb{Z}$.
2. Soit $n \in \mathbb{N}$. Si on prend $F \in \mathbb{Q}[X]$ le polynôme fournit par le Théorème VI.2.1. On prend L un corps de décomposition de F sur $\mathbb{Q}$ et on dénomme par $\alpha_1, ..., \alpha_m$ les racines de F dans L. On a que L est un corps de nombres algébriques (car $L = \mathbb{Q}[\alpha_1, ..., \alpha_m]$) et même que pour tout $i \in [\![1, m]\!]$, α_i est un entier algébrique de L.
   En effet, $F \in \mathbb{Q}[X]$ donc on peut écrire $F = \sum_{k=0}^{n} a_k X^k$, où $\forall k \in [\![0, n]\!], a_k = \frac{p_k}{q_k} \in \mathbb{Q}, (p_k, q_k) \in \mathbb{Z} \times \mathbb{Z}^*$. Donc, on pose $G = (\prod_{k=0}^{n} q_k).F \in \mathbb{Z}[X]$, et pour tout $i \in [\![1, m]\!]$ on a : $G(\alpha_i) = (\prod_{k=0}^{n} q_k).F(\alpha_i) = 0$.

On rappelle ici un Théorème qui est utilisé dans la démonstration du Lemme VI.3.6. Mais nous ne montrons pas ce Théorème, car il a peu de rapports avec le sujet.

Théorème VI.3.5 (Siegel-Mahler 1929, admis) *Pour toute courbe algébrique lisse $\mathcal{C}$ de genre $g > 0$ définie sur un corps des nombres algébriques L, dans un espace affine, il n'y a qu'un nombre fini de points sur $\mathcal{C}$ à coordonnées dans l'anneau des entiers de L.*

Lemme VI.3.6 *Soit L une extension finie de $\mathbb{Q}$ et R l'anneau des entiers de L. Soient $P_1, ..., P_m \in R[X]$ des polynômes unitaires et tels que pour un nombre premier p, aucun des P_i est une puissance de p. Alors il existe $t \in \mathbb{N}$ tel qu'aucun des $P_i(t)$ n'est une puissance de p dans L.*

Preuve (Lemme VI.3.6). Pour tout $i \in [\![1, m]\!]$, on considère la courbe $G_i : \{(x, y) \mid y^p - P_i(x) = 0\}$, il est possible de voir que cette courbe est de genre 0, mais nous ne le justifierons pas ici. Ainsi, on peut appliquer le théorème de Siegel-Mahler VI.3.5 et on obtient que pour tout $i \in [\![1, m]\!]$ la courbe G_i admet un nombre fini de points à coordonnées dans R^2. De plus on a que $\mathbb{N}^2 \subseteq R^2$ donc on a également qu'il existe un nombre fini de points de la courbe avec coordonnées dans $\mathbb{N}^2$, donc on a le résultat, car les courbes sont en nombre fini et elles contiennent tous les points qui ont pour coordonnées une racine p-ème de l'évaluation d'un P_i □

Nous pouvons donc maintenant passer à la démonstration du Théorème.

Preuve (Théorème VI.3.1). Soit G un groupe. D'après le théorème de Frucht, qui a été démontré précédemment, il existe un graphe non orienté, fini, sans boucle, connexe $X = (V, E)$ tel que $\mathrm{Aut}_{Graph}(X) \cong G$. On note $V = \{1, ..., n\}$ où $n \geq 5$ (par la preuve du théorème, il n'est pas difficile de supposer cela). On utilise le Théorème VI.2.1 pour exhiber un polynôme $F \in \mathbb{Q}[X]$ de degré n n'ayant que des racines qui sont des entiers algébriques (par la Remarque suivant la Définition VI.3.4) tel que son groupe de Galois est isomorphe à $\mathfrak{S}_n$. On prend L un corps de décomposition de F dans $\mathbb{Q}$, et on prend R l'anneau des entiers de L. On dénote maintenant par $(a_i)_{i \in [\![1,n]\!]}$ les racines de F dans L, ce sont en particulier des éléments de R. Soit $p > 3$ premier. On note $E_n = \{(i, j) \in [\![1, n]\!]^2 \mid 1 \leqslant i < j \leqslant n\}$ et on considère l'ensemble de polynômes unitaires de $R[X]$:

$$\left\{ \prod_{1 \leqslant i < j \leqslant n} (X + a_i + a_j)^{k_{i,j}} \;\middle|\; \begin{array}{c} \forall (i, j) \in E_n, k_{i,j} \in [\![0, p-1]\!] \\ \text{et } \exists (i_0, j_0) \in E_n, k_{i_0,j_0} \neq 0 \end{array} \right\}$$

Chacun de ces polynômes n'est pas une puissance de p dans $R[X]$ car on a directement une décomposition en tant que produit d'irréductibles dans $R[X]$ et on peut observer qu'aucun n'est une puissance de p dans $R[X]$. En effet, c'est évident si l'on montre que pour tous i, j, i', j', k tous différents (c'est-à-dire que le nombre de racines est plus grand que 5, ce qui est le cas) on a $a_i + a_j \neq a_{i'} + a_{j'}$. Ce qui peut se voir en faisant correspondre les indices des racines $a_i + a_j$ avec des transpositions $(i\, j)$ dans le groupe de Galois. On a que $L^{\langle (i\, j), (i'\, j') \rangle} = \{x \in L \mid \forall \sigma \in \langle (i\, j), (i'\, j') \rangle, \sigma(x) = x\}$ sur $\mathbb{Q}$ est une sous-extension de L qui contient $a_i + a_j$ mais pas $a_{i'} + a_{j'}$.

Ainsi toutes les conditions du Lemme VI.3.6 sont réunies et il existe donc un $t \in R$ tel que chacun des polynômes évalués en ce t n'est pas une puissance de p dans L.

On considère ensuite les polynômes de l'ensemble : $\{X^p - (a_i + a_j + t) \mid (i, j) \in E_n\}$ et on sait que $|E_n| = \binom{n}{2}$, ainsi on les ordonne de la façon suivante : $\{G_k \in L[X] \mid k \in [\![1, \binom{n}{2}]\!]\}$ et on prend l'ensemble $(b_k)_{k \in [\![1, \binom{n}{2}]\!]}$ tel que $\forall k \in [\![1, \binom{n}{2}]\!], b_k$ est une racine de G_k (dans la suite, on prendra pour chaque $k \in [\![1, \binom{n}{2}]\!], (i_k, j_k) \in E_n$ tel que $b_k^p = a_{i_k} + a_{j_k} + t$). On va montrer que pour tout $k \in [\![1, \binom{n}{2}]\!]$ et pour tout ε tel que $\varepsilon^p = 1$,

$$\varepsilon . b_k \notin L(b_1, ..., b_{k-1}). \tag{1}$$

En effet, supposons par l'absurde que ce n'est pas vrai, prenons $k_0 = \min\{k \in [\![1, \binom{n}{2}]\!] \mid \exists \varepsilon, \varepsilon^p = 1 \text{ et } \varepsilon . b_k \in L(b_1, ..., b_{k-1})\}$ et ε_0 tel que $\varepsilon_0^p = 1$ et $\varepsilon_0 . b_{k_0} \in L(b_1, ..., b_{k_0 - 1})$. Si $k_0 = 1$, alors $\varepsilon_0 . b_{k_0} = \gamma \in L$ et donc $(\varepsilon_0 . b_{k_0})^p = b_{k_0}^p = a_{i_{k_0}} +$

$a_{j_{k_0}} + t = \gamma^p$. Or par définition, de t par le Lemme VI.3.6, $a_{i_{k_0}} + a_{j_{k_0}} + t$ n'est pas une puissance de p dans L donc ce n'est pas possible. Si $k_0 > 1$, on a donc $\varepsilon_0.b_{k_0} \in L(b_1, ..., b_{k_0-1})$ et donc pour tout $l \in [\![1, k_0 - 1]\!]$, on applique le Lemme VI.3.3 sur le corps $L(b_1, ..., b_{l-1}, b_{l+1}, ..., b_{k_0-1}) =: L_{\hat{l}}$ avec b_l et $\varepsilon_0.b_{k_0}$ qui vérifient :

— $b_l^p = a_{i_l} + a_{j_l} + t$ donc b_l est une racine p-ème de $a_{i_l} + a_{j_l} + t$ et le polynôme $X^p - (a_{i_l} + a_{j_l} + t)$ n'a pas de racines dans $L_{\hat{l}}$ car b_l est une telle racine et les autres sont donc les $\varepsilon.b_l$ où $\varepsilon^p = 1$ qui ne sont pas dans $L_{\hat{l}}$ sinon comme $l < k_0$ cela contredirait la minimalité de k_0.

— $(\varepsilon_0.b_{k_0})^p = b_{k_0}^p = a_{i_{k_0}} + a_{j_{k_0}} + t$ donc $\varepsilon_0.b_{k_0}$ est une racine p-ème de $a_{i_{k_0}} + a_{j_{k_0}} + t$ et $\varepsilon_0.b_{k_0} \in L_{\hat{l}}(b_l)$.

Le Lemme nous dit donc qu'il existe $c_l \in L_{\hat{l}}, k_l \in \mathbb{N}, k_l < p$ tel que $\varepsilon_0.b_{k_0} = c_l.b_l^{k_l}$. Donc, on a, en regroupant le travail que l'on a fait pour chaque l, $\varepsilon_0.b_{k_0} = \gamma.\prod_{l=1}^{k_0-1} b_l^{k_l}$ où $\gamma \in L(b_1, ..., b_{k_0-1})$ mais on a également que pour tout $l_0 \in [\![1, k_0 - 1]\!]$, $\varepsilon_0.b_{k_0} = c_{l_0}.b_l^{k_{l_0}} = \gamma.\prod_{l=1}^{k_0-1} b_l^{k_l}$, donc $c_{l_0} = \gamma.\prod_{l=1, l\neq l_0}^{k_0-1} b_l^{k_l}$ et donc $\gamma \in L_{\hat{l_0}}$ et ce pour tout $l_0 \in [\![1, k_0 - 1]\!]$, donc $\gamma \in \bigcap_{l_0=1}^{k_0-1} L_{\hat{l_0}} = L$. Mais dans ce cas, on a $(\varepsilon_0.b_{k_0})^p = \gamma^p.\prod_{l=1}^{k_0-1}(b_l^{k_l})^p$ et pour tout $l \in [\![1, k_0 - 1]\!]$, b_l est racine de $X^p - (a_{i_l} + a_{j_l} + t)$, donc on a :

$$\prod_{l=1}^{k_0-1} (t + a_{i_l} + a_{j_l})^{k_l} = (\varepsilon_0.b_{k_0}\gamma^{-1})^p,$$

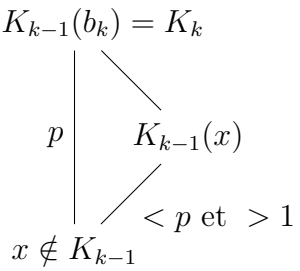
et comme $\varepsilon_0.b_{k_0}\gamma^{-1} \in L$ on a que le membre de gauche est une puissance de p dans L ce qui est impossible par définition de t par le Lemme VI.3.6. Donc finalement dans tous les cas, pour tout $k \in [\![1, \binom{n}{2}]\!]$ et $\varepsilon^p = 1$, $\varepsilon.b_k \notin L(b_1, ..., b_{k-1})$.

Ensuite, nous allons montrer par récurrence forte sur $k \in [\![0, \binom{n}{2}]\!]$, H_k : "Le corps $L(b_1, ..., b_k) =: K_k$ ne contient pas de racine p-ème de l'unité différente de 1".

— Commençons par le cas $k = 0$. Dans ce cas, on voit que tout devient évident si p est choisi tel que $p - 1 > n!$, or aucune condition sur p n'est exigé si ce n'est qu'il soit premier, donc par l'infinitude des nombres premiers, on peut prendre un p qui convient à notre condition et dans ce cas il n'y a pas, dans $L/\mathbb{Q}$ (de degré divisant $n!$), de racine p-ème de l'unité si ce n'est 1.

— Soit $k \in [\![0, \binom{n}{2}]\!]$. Supposons que pour tout $m < k$, la propriété H_m est vérifiée. On a que $K_k = K_{k-1}(b_k)$ et on sait que : $b_k^p - (a_i + a_j + t) = 0$, donc b_k est une racine de $X^p - (a_i + a_j + t) \in L[X] \subseteq K_{k-1}[X]$, ainsi le degré de b_k est 1 ou p sur K_{k-1}. Or $1^p = 1$ donc par ce qu'on a fait précédemment en (1), on a que $1.b_k = b_k \notin K_{k-1}$, donc le degré de b_k sur K_{k-1} est égal à p.

Supposons maintenant qu'il existe $x \in K_k$ tel que $x \neq 1$ et $x^p = 1$.



Le degré de x sur K_{k-1}, qui est $[K_{k-1}(x) : K_{k-1}]$, est strictement supérieur à 1 car $x \in K_{k-1}(x)$ mais $x \notin K_{k-1}$, ainsi $K_{k-1} \subsetneq K_{k-1}(x)$. De plus $X^p - 1 = (X-1)(X^{p-1} + ... + X + 1)$, or x est racine de $X^p - 1$ et comme $x \neq 1$ on a que x est racine de $X^{p-1} + ... + X + 1$, donc $[K_{k-1}(x) : K_{k-1}] < p$. De plus, par multiplicativité des degrés, on a que $[K_{k-1}(x) : K_{k-1}] | [K_k : K_{k-1}]$ ce qui est impossible et donc on en déduit qu'il n'existe pas de $x \in K_k$ tel que $x \neq 1$ et $x^p = 1$. Et donc on a obtenu H_k. □

On conclut donc par récurrence.

Il nous reste donc plus qu'à construire l'extension K_G de l'énoncé. On considère $\{b_k \mid k \in [\![0, \binom{n}{2}]\!] \wedge \exists [i,j] \in E, b_k^p = a_i + a_j + t\}$, on note m le cardinal de cet ensemble (remarquons $m \leq |E|$) et on renomme les éléments de cet ensemble en : $c_1, ..., c_m$ (les c_i jouent donc le même rôle que les b_i à permutation près, mais dans tous les cas ils ont les mêmes propriétés que ce que l'on a vu pour les b_i précédemment). On pose ensuite $K_G = L(c_1, ..., c_m) = \mathbb{Q}(a_1, ..., a_n, c_1, ..., c_m)$. Montrons maintenant que $\mathrm{Aut}_{Graph}(X) \cong \mathrm{Aut}_{extension}(K_G/\mathbb{Q})$.

Soit $\psi \in \mathrm{Aut}_{Graph}(X)$. On prend le morphisme d'extension :

$$\varphi : \begin{array}{ccc} L & \to & L \\ a_i & \rightsquigarrow & a_{\psi(i)}, \forall i \in V, \end{array}$$

φ est construit en appliquant le Théorème de prolongement des isomorphismes VI.2.8 appliqué, un à un, à chaque a_i, racine de F irréductible sur $\mathbb{Q}$ et en prolongeant $id_{\mathbb{Q}}$. Grâce à ce procédé, on obtient d'abord naïvement un plongement de $L/\mathbb{Q}$ mais on remarque que son image est incluse dans L donc on en déduit facilement que φ est un automorphisme et de plus par l'unicité dans le Théorème de prolongements des isomorphismes, on a que φ est unique. On va maintenant prolonger φ à tout K_G. On sait que c_1 est racine de $X^p - (a_{i_1} + a_{j_1} + t)$ qui est un polynôme irréductible par la Proposition VI.3.2, car n'a pas de racine dans L, en effet, s'il y avait une racine $x \in L$ alors les autres racines serait les éléments de $\{\varepsilon.x \mid \varepsilon^p = 1\}$ et donc $c_1 = \varepsilon_0.x$ avec $\varepsilon_0^p = 1$, or on a vu précédemment en (1) que $\varepsilon_0.c_1 \notin L$, ce qui est absurde. On peut donc appliquer encore une fois le théorème de prolongement des isomorphismes avec φ, le polynôme irréductible $X^p - (a_{i_1} + a_{j_1} + t)$ et la racine c_1 et on sait qu'il existe une unique morphisme $\varphi_1 : L(c_1) \to \overline{L}$ qui prolonge φ et tel que c_1 est envoyé sur une racine de $\varphi(X^p - (a_{i_1} + a_{j_1} + t)) = X^p - (a_{\psi(i_1)} + a_{\psi(j_1)} + t)$. De plus on sait qu'il existe $m_0 \in [\![1, m]\!]$ tel que c_{m_0} est une racine de $X^p - (a_{\psi(i_1)} + a_{\psi(j_1)} + t)$ et on sait que c'est la seule, car les autres racines sont les $\varepsilon^k.c_{m_0}$ mais on a vu que dans $L(b_1, ..., b_{\binom{n}{2}})$ il n'y avait que 1 comme racine de p donc forcément $c_1 \overset{\varphi_1}{\rightsquigarrow} c_{m_0}$, on peut résumer cela en $\sqrt[p]{a_{i_1} + a_{j_1} + t} \overset{\varphi_1}{\rightsquigarrow} \sqrt[p]{a_{\psi(i_1)} + a_{\psi(j_1)} + t}$ (car on a à chaque fois 1 seule racine p-ème dans les corps considérés). De la même manière, on fait la même étude pour $c_2, ..., c_m$ et on a donc :

$$\widetilde{\varphi} : \begin{array}{rcl} K_G & \to & K_G \\ a_i & \rightsquigarrow & a_{\psi(i)}, \forall i \in V \\ \sqrt[p]{a_{i_1} + a_{j_1} + t} & \rightsquigarrow & \sqrt[p]{a_{\psi(i_1)} + a_{\psi(j_1)} + t}, \forall i \in V \end{array}$$

qui est un automorphisme et on sait qu'un morphisme d'extension avec ces conditions est unique. Pour chaque $\psi \in \mathrm{Aut}_{Graph}(X)$ on a donc défini $\varphi_\psi \in \mathrm{Aut}_{extensions}(K_G)$.

Soit $\varphi \in \mathrm{Aut}_{extension}(K_G)$. Pour tout $i \in V$, a_i est une racine de F qui est donc envoyé sur une autre racine de F, ainsi il existe $j \in V$ tel que $\varphi(a_i) = a_j$. On définit donc $\psi : V \to V$ tel que $\forall i \in V, \varphi(a_i) = a_{\psi(i)}$, c'est une bijection. Montrons que ψ est un morphisme. Soient $[i,j] \in E$, alors par construction des $(c_k)_k$ il existe un c_{k_0} tel que $(c_{k_0})^p = a_i + a_j + t$, donc $\sqrt[p]{a_i + a_j + t} \in K_G$ qui est envoyé sur un élément de K_G. De plus, on a que $\sqrt[p]{a_i + a_j + t}$ est racine de $X^p - (a_i + a_j + t)$ et est donc envoyé sur une racine de $\varphi(X^p - (a_i + a_j + t)) = X^p - (a_{\psi(i)} + a_{\psi(j)} + t)$ donc de la forme $\varepsilon.\sqrt[p]{a_{\psi(i)} + a_{\psi(j)} + t}$ avec $\varepsilon^p = 1$, qui est donc un $\varepsilon.c_{m_0}$ pour $m_0 \in [\![1, m]\!]$. Mais on sait que dans K_G il n'y a que 1 comme p-ème de l'unité. Ainsi $\sqrt[p]{a_i + a_j + t} \overset{\varphi_1}{\rightsquigarrow} \sqrt[p]{a_{\psi(i)} + a_{\psi(j)} + t}$, donc $[\psi(i), \psi(j)] \in E$ et ainsi ψ est un automorphisme de $K_G/\mathbb{Q}$. Et donc pour tout $\varphi \in \mathrm{Aut}_{extension}(K_G)$ on peut définir $\psi_\varphi \in \mathrm{Aut}_{Graph}(X)$.

On peut donc définir :

$$\chi : \begin{array}{ccc} \mathrm{Aut}_{Graph}(X) & \to & \mathrm{Aut}_{extension}(K_G) \\ \psi & \mapsto & \varphi_\psi \end{array},$$

$$\phi : \begin{array}{ccc} \mathrm{Aut}_{extension}(K_G) & \to & \mathrm{Aut}_{Graph}(X) \\ \varphi & \mapsto & \psi_\varphi \end{array}.$$

On vérifie de même que $\chi \circ \phi = Id_{\mathrm{Aut}_{extension}(K_G)}$ et $\phi \circ \chi = Id_{\mathrm{Aut}_{Graph}(X)}$. Donc on a finalement $\mathrm{Aut}_{Graph}(X) \cong \mathrm{Aut}_{extension}(K_G/\mathbb{Q})$. Ce qui termine la preuve.

VII Espaces topologiques

Definition VII.0.1 (Topologie) Soit E un ensemble. On appelle *topologie* sur E, un ensemble $\mathcal{T}$ de parties de E vérifiant les propriétés suivantes :

1. $\emptyset, E \in \mathcal{T}$
2. Si $(O_i)_{i \in I} \in \mathcal{T}^I$ est une famille quelconque d'éléments de $\mathcal{T}$, où I est un ensemble quelconque, alors $\bigcup_{i \in I} O_i \in \mathcal{T}$.
3. Si $(O_i)_{i \in [\![1,N]\!]} \in \mathcal{T}^I$ est une famille finie d'éléments de $\mathcal{T}$, alors $\bigcap_{i=1}^N O_i \in \mathcal{T}$

Un *espace topologique* est un couple $(E, \mathcal{T})$, où E est un ensemble et $\mathcal{T}$ est une topologie sur E.

Definition VII.0.2 (Continuité) Soient $(X, \mathcal{T}_X)$ et $(Y, \mathcal{T}_Y)$ deux espaces topologiques et $f : X \to Y$ une application. On dit que f est *continue* si toute image réciproque d'un ouvert de Y est un ouvert de X, c'est-à-dire : $\forall O \in \mathcal{T}_X, f^{-1}(0) \in \mathcal{T}_Y$.

Remarque: On peut donc définir une catégorie sur la classe des espaces topologiques (notée $Topo$), les morphismes de cette catégorie sont les homéomorphismes définis ci-dessous :

Definition VII.0.3 (Homéomorphisme) Soient $(X, \mathcal{T}_X)$ et $(Y, \mathcal{T}_Y)$ deux espaces topologiques et $f : X \to Y$ une application. On dit que f est un *homéomorphisme* si f continue, f bijective et f^{-1} continue. Un homéomorphisme de X dans X est appelé un *autohoméomorphisme* et l'ensemble des autohoméomorphisme sera noté $\mathrm{Aut}_{Topo}(X)$

Definitions VII.0.4 (Métrique) Soit M un ensemble non vide. Une *distance* sur M est une application $d : M \times M \to \mathbb{R}_+$ qui vérifie :

— Symétrie : $\forall x, y \in M, d(x, y) = d(y, x)$

— Séparation : $\forall x, y \in M, d(x, y) = 0 \Leftrightarrow x = y$

— Inégalité triangulaire : $\forall x, y, z \in E, d(x, y) \leqslant d(x, z) + d(z, y)$

Le couple (M, d) est alors appelé un *espace métrique*.

Remarque: Il serait "fou" de dire que nous avons présenté tout ce qu'il y a à dire sur les espaces topologiques avec les 4 définitions ci-dessous, malheureusement nous n'entreront pas plus dans les détails de l'étude de ces espaces et nous considérerons comme acquis beaucoup de résultat sur ces espaces. Comme par exemple le fait qu'un espace métrique est topologique.

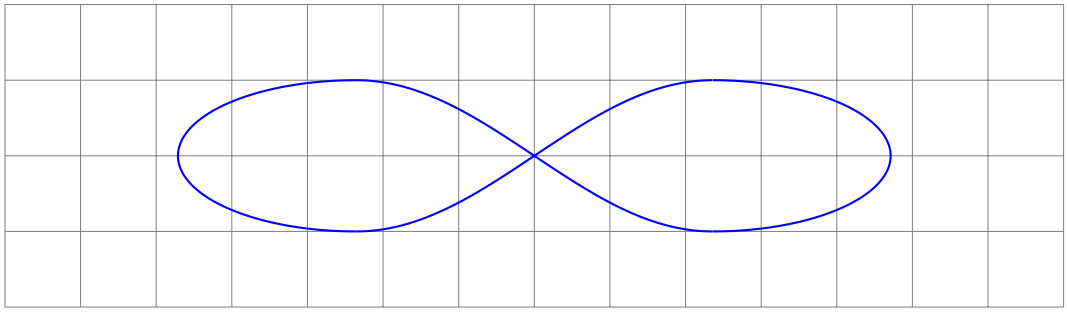
L'objectif de cette section est de présenter une construction d'espace topologique (en particulier ici métrique) qui serait en mesure de démontrer le théorème suivant. Nous ne ferons pas les preuves ici, mais le lecteur pourra trouver une étude plus complète avec la source [5].

Théorème VII.0.5 *Soit G un groupe fini. Il existe un espace topologique $(X, \mathcal{T}_X)$ tel que $\mathrm{Aut}_{Topo}(X) \cong G$.*

Nous allons même faire un peu mieux en montrant qu'il existe un espace métrique compact connexe composé de courbe de Peano dont nous décrivons la construction ci-dessous :

Construction : On commence par considérer un disque ouvert du plan : $\mathbb{D} = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leqslant 1\}$. On sait que $\mathbb{Q}^2$ est dénombrable et dense dans $\mathbb{R}^2$ donc $C := \overset{\circ}{\mathbb{D}} \cap \mathbb{Q}^2$ est une partie dénombrable dense dans $\overset{\circ}{\mathbb{D}}$ (et aussi $\mathbb{D}$). On note donc $C = \{a_i \mid i \in \mathbb{N}^*\}$. On va définir une suite d'hélices dans $\mathbb{D}$. On entend par hélice une courbe par exemple composé de deux ou plusieurs ailes, on pourra avoir en tête pour le cas de deux ailes la courbe suivante ou plutôt une déformation de celle-ci :

$$\left\{\begin{array}{ccc} [-2\pi, 2\pi] & \to & \mathbb{R}^2 \\ \theta & \mapsto & \left\{\begin{array}{ll} (3(\cos(\theta + \frac{5\pi}{2}) - sign(\theta + \frac{5\pi}{2})), \sin(\theta + \frac{5\pi}{2})) & \text{sur } [-2\pi, -\pi], \\ (\frac{3}{2}(\theta + \frac{\pi}{2}), \sin(\theta + \frac{\pi}{2})) & \text{sur } [-\pi, 0], \\ (\frac{3}{2}(\theta - \frac{\pi}{2}), -\sin(\theta - \frac{\pi}{2})) & \text{sur } [0, \pi], \\ (3(\cos(\theta - \frac{3\pi}{2}) + sign(\theta - \frac{3\pi}{2})), \sin(\theta - \frac{3\pi}{2})) & \text{sur } [\pi, 2\pi]. \end{array}\right. \end{array}\right.$$



On ajoutera des ailes de la même forme pour les hélices avec plus d'ailes.

On commence pour $i = 1$, on place au point a_1 une courbe hélice α_1 avec 3 ailes, centrée sur a_1, qui est incluse dans $\mathbb{D}$ et dans la boule ouverte de centre a_1 et de rayon 1 notée $B(a_1, 1)$. On procède ensuite par induction. Supposons que les $n-1$ premières courbes hélices ont été construites et on prend a'_n le premier élément de C (donc qui ne fait pas partie du bord de $\mathbb{D}$) qui ne fait pas partie de l'intérieur d'une courbe hélice ni du bord de ces hélices et on place, centrée en a'_n, une hélice possédant $n+2$ ailes, qui ne touche pas l'intérieur des autres hélices déjà construites et qui est incluse dans la boule ouverte centrée en a'_n et de rayon $1/n$ notée $B(a'_n, 1/n)$, ce qui est toujours possible, car les hélices sont des courbes dont le bord et l'intérieur forme un compact à l'intérieur de $\mathbb{D}$ le disque fermé donc en enlevant ces compacts on obtient toujours un ouvert. On définit donc l'espace P comme étant $\mathbb{D}$ privé de tous les intérieurs des hélices (et non la courbe qui forme le bord de l'hélice).

On a que P et un espace métrique (hérité de la métrique sur $\mathbb{R}^2$), compact et connexe comme intersection décroissante d'espaces compacts et connexes. De plus P est un espace de dimension 1, car il ne contient pas d'ouvert du plan (la famille C étant dense, à proximité de chaque point de P se trouve une hélice).

Definition VII.0.6 Soit $(E, \mathcal{T})$ un espace topologique, on dit qu'il est *rigide* si $\mathrm{Aut}_{Topo}(E) = \{id_E\}$.

Proposition VII.0.7 *La courbe de Peano P est rigide.*

Preuve. Idée de preuve :

Il s'agit d'étudier localement les composantes connexes de tous les points de P, pour se rendre compte que les points qui ont un nombre de composantes connexes (de P privé du point) plus grand qu'une certaine constante sont les centres "a_i" des hélices dans la construction de P et que, de plus, chacun d'entre eux a un nombre différent de composantes connexes localement et un nombre supérieur à la constante de départ. Ainsi l'étude des espaces connexes nous dit que ces points de P qui sont des centres "a_i" sont fixés par tout homéomorphisme de P dans P et ceux-ci étant dense dans P on en déduit que tout homéomorphisme fixe tout point de P. Donc que P est rigide. □

Preuve (Théorème VII.0.5). Idée de preuve :

Soit G un groupe fini. On considère pour tout $g \in G$ une copie d'une courbe de Peano P que l'on notera R_g.

On raisonne donc de la même manière que pour la démonstration du théorème de Frucht en considérant non pas des graphes rigides, mais des espaces rigides qui sont les copies des courbes de Peano R_g. On considère tout d'abord dans les R_g deux points h_0, h_1 qui sont le plus éloignés possible (on peut voir qu'ils sont à distance 1). Puis, on prend $X = (V, E)$ le graphe non orienté du Théorème III.5.1 associé à G et on remplace chaque arête $[x, y] \in E$ par un espace R_g différent où on connecte x à h_O et y à h_1. Notons $\mathcal{M}$ l'espace obtenu. Finalement il reste juste à voir que l'image par un homéomorphisme d'un R_g en tant que sous-espace de $\mathcal{M}$ est un autre R_h, ce qui se voit en étudiant les propriétés topologiques des voisinages des "sommets du graphe" de $\mathcal{M}$. Si on a prouvé ceci, alors on peut faire complètement correspondre les morphismes de graphes qui préservent les graphes rigides "H_k" de la démonstration du Théorème de Frucht et les homéomorphismes de $\mathcal{M}$ qui, eux,

préservent les sous-graphes copie des courbes de Peano (aussi rigide). Donc, on en déduit que $Aut_{Topo}(\mathcal{M}) \cong G$. □

Remarque: Les idées de preuves données ci-dessus ne représentent, malheureusement, même pas la prémisse d'une preuve tant les détails manquants sont nombreux. Elles ont simplement le mérite de présenter en quoi le Théorème de Frucht est central dans ces constructions.

VIII Foncteurs & Conclusion

Dans cette section, nous allons résumer les résultats obtenus lors de notre étude et introduire la notion de foncteur afin de comprendre un peu mieux ce mécanisme de la théorie des catégories qui apparait en fait dans certaines démonstrations.

VIII.1 Foncteurs

Tout d'abord, énonçons la définition d'un foncteur.

Definition VIII.1.1 (Foncteur) Soient $\mathcal{C}, \mathcal{D}$ deux catégories. Un foncteur $F : \mathcal{C} \to \mathcal{D}$ est la donnée de deux fonctions F_{ob} et F_{mor}, où :

- F_{ob} associe à tout objet X de $\mathcal{C}$, un objet $F_{\text{ob}}(X)$ de $\mathcal{D}$,
- F_{mor} associe à tout morphisme $f : X \to Y$ de $\mathcal{C}$, un morphisme $F_{\text{mor}}(f) : F_{\text{ob}}(X) \to F_{\text{ob}}(Y)$ de $\mathcal{D}$,

et telles que F_{ob} et F_{mor} :

- respectent les identités : pour tout objet X de $\mathcal{C}$, $F_{\text{mor}}(id_X) = id_{F_{\text{ob}}(X)}$,
- respectent la composition : pour tous objets X,Y et Z et tous morphismes $f : X \to Y$ et $g : Y \to Z$ de $\mathcal{C}$,

$$F_{\text{mor}}(g \circ f) = F_{\text{mor}}(g) \circ F_{\text{mor}}(f).$$

La première apparition d'un foncteur se situe dans la démonstration du Théorème III.5.1 de Frucht. En effet, lors de cette démonstration, nous avons pris le graphe coloré orienté $\mathcal{C}(G)$ de Cayley d'un groupe G et nous l'avons fait correspondre avec un graphe non orienté $\widehat{\mathcal{C}(G)}$ qui remplaçait chaque arête colorée orientée par un type de sous-graphe "H_k". Cette construction peut se généraliser, en effet si l'on se fixe $\mathcal{A}$ un ensemble de couleurs (et donc on fixe la catégorie $Couleur_{\mathcal{A}}$, dans le cas de la construction $\mathcal{A}$ doit être dénombrable, mais nous avons vu que ce n'était pas forcément nécessaire dans le Théorème V.0.1 de Sabidussi) alors pour tout graphe X coloré orienté le fait de remplacer les arêtes par des sous-graphes non orientés correspondants peut également se faire et construire un graphe $\widehat{X}$ de la catégorie $Graph$. De plus, nous avons vu qu'à tout morphisme α de $\mathcal{C}(G)$ préservant la couleur, on pouvait faire correspondre $\widehat{\alpha}$ un unique morphisme de $\widehat{\mathcal{C}(G)}$ par notre construction, ceci se généralise de la même façon et à tout morphisme α d'un graphe de $Couleur_{\mathcal{A}}$ on peut faire correspondre $\widehat{\alpha}$ de la même manière. Ainsi, on définit un foncteur par :

$$\begin{array}{ccc} Couleur_{\mathcal{A}} & \longrightarrow & Graph \\ X & \overset{\text{ob}}{\longmapsto} & \widehat{X} \\ \alpha & \overset{\text{mor}}{\longmapsto} & \widehat{\alpha}. \end{array}$$

De la même manière, il doit être possible de fabriquer un foncteur $Graph \longrightarrow Topo$ grâce à la construction de la section VII. Par contre, dans la section VI qui traite des extensions de $\mathbb{Q}$, il n'y a pas moyen de construire un foncteur de manière évidente avec la démonstration, car nous utilisons dans la construction les racines d'un polynôme F tel que son groupe de Galois est $\mathfrak{S}_n$, cependant cette construction ne peut pas être la même pour tout graphe.

Finalement, à titre d'autre exemple, on peut revenir sur les définitions de graphe orienté et non orienté. Nous avons défini les graphes non orientés comme étant des graphes orientés pour lequel, pour chaque arête orienté il existe la même arête dans l'autre sens. Nous pourrions modifier cette définition pour définir les graphes non orientés munis d'arêtes, mais qui n'ont pas de sens. On peut donc définir un foncteur entre cette nouvelle catégorie et la catégorie précédemment définie des graphes qui fait correspondre les graphes non orientés et les graphes de $Graph$ qui ont une arête de chaque sens pour chaque arête.

VIII.2 Tableau résumé

Nous allons finir cette section par un tableau récapitulatif des catégories sur lesquelles nous pouvons répondre au problème de la réalisabilité de groupes.

Réalise les groupes	Ne réalise pas les groupes
$Couleur_{\mathcal{A}}$	Grp
$Graph$	Ord
$Extensions_{\mathbb{Q}}$	$Extensions_{\mathbb{F}_q}$
$Topo$	Set

On remarquera que la section V montre même que la catégorie $Graph$ réalise tous les groupes, même ceux d'ordre infini et que la construction du graphe de Cayley n'est pas spécifié comme étant réservé aux graphes finis, ainsi $Couleur_{\mathcal{A}}$ et $Graph$ réalisent tous les groupes, même ceux d'ordre infini.

Pour les extensions de $\mathbb{F}_q$, un corps fini, le Lemme VI.2.11 nous dit que le groupe de Galois (le groupe d'automorphismes) d'une extension d'un corps fini est cyclique. Or il existe des groupes non cycliques, donc $Extensions_{\mathbb{F}_q}$ ne réalise pas les groupes.

Finissons par ce par quoi nous avons commencé : la catégorie Set des ensembles. Soit E un ensemble. On rappelle que les isomorphismes pour cette catégorie sont les bijections et les automorphismes forme bien un groupe qui n'est nul autre que $\mathfrak{S}(E)$ le groupe symétrique. Or tout groupe fini n'est pas en groupe symétrique, donc en particulier Set ne réalise pas tous les groupes.

Références

[1] Gregory Berhuy. *Algèbre : le grand combat*. T. 121. Mathématiques en devenir. Calvage et Mounet, 2018, p. 785-970. ISBN : 9782916352664. URL : https://books.google.fr/books?id=lJzSswEACAAJ.

[2] Nicolas Bourbaki. *Théorie des ensembles*. 1970, E III.47. DOI : https://doi.org/10.1007/978-3-540-34035-5.

[3] Patrick Dehornoy. *Chapitre 2 : Les ordinaux*. Notes de cours : Logique et théorie des ensembles. 2006. URL : https://www.lmno.cnrs.fr/archives/dehornoy/Surveys/DehornoyChap2.pdf.

[4] E. Fried et J. Kollár. "Automorphism groups of algebraic number fields". In : *Mathematische Zeitschrift* 163 (1978), p. 121-123. DOI : https://doi.org/10.1007/BF01214058.

[5] J. de Groot. "Groups represented by homeomorphism groups I". In : *Mathematische Annalen* 138 (1959), p. 80-102. DOI : https://doi.org/10.1007/BF01369667.

[6] J. de Groot et R.J. Wille. "Rigid continua ant topological group-picture". In : *Archiv der Mathematik* IX (1958), p. 441-446. DOI : https://doi.org/10.1007/BF02230943.

[7] Kato Makoto. *Constructing a Galois extension field with Galois group S_n*. Mathematics Stack Exchange. URL : https://math.stackexchange.com/q/166872.

[8] Damiano Mazza. *Introduction à la théorie des catégories*. Notes de cours. 2019. URL : https://lipn.univ-paris13.fr/~mazza/teaching/IntroCat.pdf.

[9] Ore Oystein. *Theory of Graphs*. T. XXXVIII. 1962, p. 239-245. DOI : http://dx.doi.org/10.1002/andp.19053221004.

[10] Gert Sabidussi. "Graphs with given infinite group". In : *Monatshefte für Mathematik* 64 (1960), p. 64-67. DOI : https://doi.org/10.1007/BF01319053.