Le Grand Théorème de Fermat
Livre 02 - Groupes
Version 2.0

Pascal Picard*

18 janvier 2010

*Je suis grand amateur de Mathématiques et de Physique Théorique, convaincu que ces sciences sont accessibles à tous, à condition de les expliquer progressivement et méthodiquement, et de les introduire par les prérequis nécessaires. Depuis quelques années, je m'attèle à écrire des textes théoriques sous forme de pièces de théâtre. Trois personnages y bavardent : Béatrix est la Candide, c'est elle qui pose les questions ; Euristide est un peu philosophe, un peu physicien, il est l'intuitif du groupe ; Mathine est notre mathématicienne, c'est elle qui présente les calculs et les démonstrations. Ces textes sont mis à disposition gratuitement sur Internet, parce que j'aime ça. Le prérequis pour la lecture des documents, quelque complexes qu'ils soient, est le programme de Terminale S en France.

à Pascale, Marine et Morgane

Remerciements... Ce document est en phase de relecture. Les relecteurs motivés recevront mes remerciements chaleureux.

Table des matières

Table des figures

Résumé

`BEATRIX` : La théorie des groupes... C'est un peu mystérieux. Qu'est-ce donc ?

`EURISTIDE` : Les groupes sont des objets qui permettent de structurer des ensembles pour faire apparaître leur symétrie. Les groupes nous accompagnent, sans que nous le sachions bien souvent, tous les jours de notre vie. Quand vous regardez l'heure, vous observez en fait une structure de groupe. Quand vous faites une addition, c'est encore dans une structure de groupe. Si vous jouez au Rubik's cube, vous faites un bel exercice de théorie des groupes.

`MATHINE` : Si la théorie des groupes est omniprésente, c'est parce qu'elle constitue une des structures fondamentales des mathématiques. La grande majorité des structures s'appuient en effet sur celle des groupes.

1 Acte - Introduction

EURISTIDE : La théorie des groupes constitue le premier grand chapitre de l'Algèbre moderne. La structure de groupe est en effet omniprésente en Algèbre et sert de fondations pour la création de structures plus élaborées telles que les Anneaux, les Corps et les Espaces Vectoriels.
Nous commencerons notre discussion par une présentation des relations d'équivalence. Ceci nous permettra de dégager la notion d'ensemble quotient. Puis nous verrons les relations d'ordre dont nous conclurons l'exposé par la présentation du célèbre Lemme de Zorn. Nous pourrons alors construire la structure de groupe et ses premières propriétés. Viendra ensuite la structuration des sous-ensembles d'un groupe sous forme de sous-groupe. Les homomorphismes nous permettront de mettre en relation des groupes, et en particulier de transporter une structure de groupe d'un ensemble sur un autre. Nous verrons alors comment les groupes peuvent être engendrés à partir d'un élément, ou d'un ensemble d'éléments. Nous comprendrons alors ce qui caractérise un groupe fini ou des entités telles que groupes monogènes et groupes cycliques. Nous construirons ensuite la structure de groupe quotient. Ce sera l'opportunité de présenter les sous-groupes distingués et les trois théorèmes d'isomorphisme. Nous aborderons ensuite le concept d'action d'un groupe sur un ensemble. Et pour finir, nous établirons le lien important qui existe entre les sous-groupes d'un groupe fini et les nombres premiers, dans le cadre de l'étude des p-groupes et des p-Zylow ; ceci nous permettra de comprendre en particulier dans quelle mesure la théorie des nombres possède des attaches fondamentales avec la structure de groupe.

BEATRIX : C'est un menu assez copieux, mais je me délecte d'avance.

2 Acte - Relations d'équivalence

2.1 Scène - Relations d'équivalence

EURISTIDE : Pour commencer l'étude des groupes, nous allons donc commencer par présenter la notion de relation d'équivalence et de relation d'ordre.

BEATRIX : Mais qu'est-ce qu'une relation, d'abord ?

EURISTIDE : Oui, tu as raison, Béatrix. Commençons donc par définir ce qu'est une relation. Il faut considérer une relation entre deux éléments d'un ensemble, comme une propriété qui relie ces deux éléments. L'égalité, par exemple, est une relation : "L'âge de Paul est égal à l'âge d'Eric". La supériorité en taille est une relation : "Paul est plus grand que Pierre". Commençons par définir quelques types particuliers de relations.

MATHINE : Définissons en premier lieu la réflexivité.

Définition **2.1.1**
Relation réflexive
Une relation $\mathcal{R}$ sur un ensemble X est réflexive si pour tout $x \in X$, elle vérifie $x\mathcal{R}x$.

EURISTIDE : Les relations réflexives sont ainsi des relations dont tous les objets sont en relation avec eux-mêmes. Ce relations représentent souvent des relations d'égalité, d'appartenance à une caractéristique commune, etc.
Le schéma ci-après symbolise une telle relation.

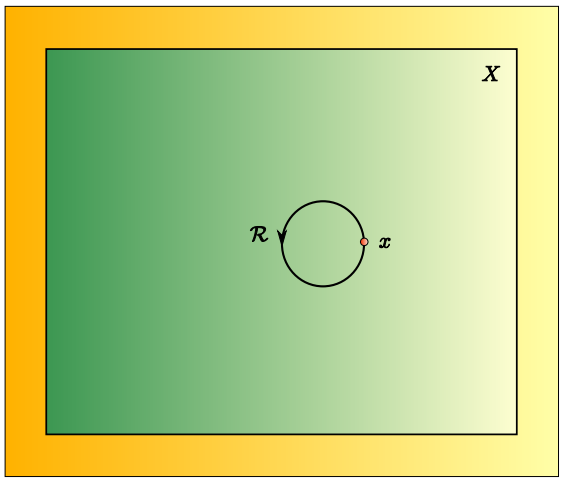

Fig. 1 - Relation réflexive

Béatrix, peux-tu me donner un exemple simple de relation réflexive ?

BEATRIX : La relation "est égal à". x est bien évidemment égal à lui-même.

EURISTIDE : Il y en a d'autres. La relation "est supérieur ou égal à" ou la relation "est de la même famille que".

MATHINE : Voyons maintenant un autre type de relations.

Définition **2.1.2**
Relation symétrique
Une relation $\mathcal{R}$ sur un ensemble X est symétrique si pour tout x et y appartenant à X, lorsqu'elle vérifie $x\mathcal{R}y$, alors elle vérifie $y\mathcal{R}x$.

EURISTIDE : Les relations symétriques, comme leur nom l'indique, sont des relations qui s'appliquent aux objets dans les deux sens.

BEATRIX : Cela veut-il dire que nous avons le schéma suivant ?

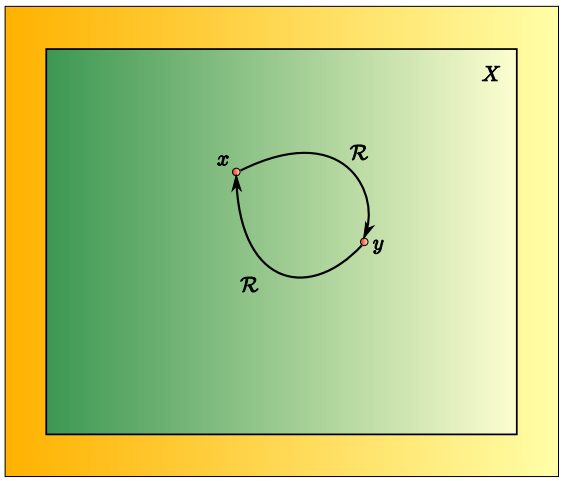

Fig. 2 - Relation symétrique

EURISTIDE : Oui, tout à fait. Ces relations représentent aussi souvent des relations d'égalité ou d'appartenance à une famille commune.

BEATRIX : J'ai en tête quelques exemples. La relation "est égal à" est symétrique bien sûr. Mais aussi "est le frère de", ou "est de la famille de".

EURISTIDE : En revanche, la relation "est strictement supérieur à" n'est pas symétrique, puisque si x est strictement supérieur à y, alors y ne peut pas être strictement supérieur à x.

MATHINE : Continuons la présentation des types de relations.

Définition **2.1.3**
Relation transitive
Une relation $\mathcal{R}$ sur un ensemble X est transitive si pour tout x, y et z appartenant à X, elle vérifie ($x\mathcal{R}y$ et $y\mathcal{R}z$) $\Rightarrow$ $x\mathcal{R}z$.

EURISTIDE : Les relations transitives, comme cela est suggéré par leur nom, se transmettent de proche en proche. Elles correspondent souvent à des relations d'ordre ou d'égalité, ou d'appartenance à une famille commune.

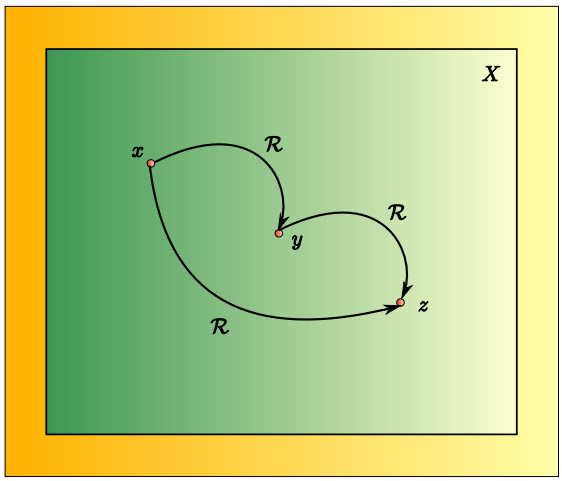

Fig. 3 - Relation transitive

Par exemple, les relations suivantes sont transitives : "est égal à", "est supérieur ou égal à", "est de la famille de".

BEATRIX : D'accord, je retiens donc : relation transitive = relation qui se transmet de proche en proche.

MATHINE : Nous allons maintenant aborder la notion essentielle de relation d'équivalence. Nous verrons que c'est un concept omniprésent en mathématiques, et nous en ferons un usage intensif.

Définition **2.1.4**
Relation d'équivalence
Une relation $\mathcal{R}$ sur un ensemble X est dite relation d'équivalence si elle est réflexive (cf. 2.1.1), symétrique (cf. 2.1.2) et transitive (cf. 2.1.3).

EURISTIDE : La relation d'équivalence est à considérer comme une relation liant les objets ayant une caractéristique commune. Les objets ayant une propriété commune se trouvent donc mis en relation par la relation d'équivalence.

BEATRIX : J'aimerais comprendre la raison d'être des propriétés de cette relation d'équivalence : réflexivité, symétrie, transitivité.

EURISTIDE : La réflexivité permet d'assurer que les objets sont "équivalents" à eux-mêmes. La symétrie

permet de garantir que des éléments équivalents entre eux le sont bien "dans les deux sens" ; en effet, une équivalence dans un seul sens n'aurait que peu de signification intuitive. Et la transitivité nous assure que la relation se propage "de proche en proche", veillant à ce que les éléments indirectement en relation par l'intermédiaire d'un ou plusieurs éléments, sont mis en relation directement grâce à cette transitivité.

BEATRIX : Un peu comme "les amis de mes amis sont mes amis".

EURISTIDE : Oui, la relation "est l'ami de" peut être considérée comme une relation d'équivalence, sous réserve que nous vivions dans un monde où :
- Chacun est son propre ami ;
- Ne sont amies que des personnes partageant cette amitié entre elles réciproquement. Pierre ne peut pas être l'ami de Paul, si Paul n'est pas l'ami de Pierre ;
- Si l'adage "les amis de mes amis sont mes amis" est bien respecté.

Comme tu le vois, je viens d'énoncer les propriétés d'une relation d'équivalence pour cette relation "est l'ami de".

BEATRIX : J'ai des exemples assez immédiats de relations d'équivalence : "est égal à", ou "est de la famille de".

EURISTIDE : Les relations d'équivalence, compte tenu de leurs propriétés de symétrie et de transitivité, permettent de grouper les éléments qui sont en relation entre eux dans des ensembles d'éléments tous en relation entre eux.

MATHINE : C'est ce qui va nous permettre de définir les classes d'équivalence.

Définition **2.1.5**
Classe d'équivalence
Soit X un ensemble muni d'une relation d'équivalence (cf. 2.1.4) $\mathcal{R}$. Soit x un élément de X. On appelle classe d'équivalence de x suivant $\mathcal{R}$ l'ensemble $\{y \in X ; y\mathcal{R}x\}$.

EURISTIDE : Les classes d'équivalence illustrent bien cette notion de "famille". Tous les membres d'une même famille qui sont en relation entre eux par une relation d'équivalence, appartiennent à cet ensemble commun appelé classe d'équivalence.

BEATRIX : Je comprends bien. Par exemple, pour la relation "est de la famille de", les classes d'équivalence sont les familles, justement.

MATHINE : Cette remarque nous conduit naturellement à la notion de représentant d'une classe.

Définition **2.1.6**
Représentant d'une classe d'équivalence
Un élément d'une classe d'équivalence (cf. 2.1.5) est appelé représentant de la classe d'équivalence.

EURISTIDE : Ainsi, dans l'exemple de la relation "est de la famille de", le nom de "représentant" est tout à fait judicieux, puisque chaque élément d'une classe d'équivalence (en l'occurrence, ici une famille) est précisément souvent appelé un représentant de la famille.

BEATRIX : C'est vrai. La famille de Paul est une classe d'équivalence. Et si Pierre est le frère de Paul, alors Paul et Pierre sont deux représentants de cette famille.

MATHINE : Nous allons maintenant noter une première proposition très simple des classes d'équivalence.

Proposition **2.1.1**
Non vacuité d'une classe d'équivalence
Une classe d'équivalence (cf. 2.1.5) n'est pas vide.

EURISTIDE : Intuitivement, si la famille de Paul est définie, c'est que Paul au moins s'y trouve. On fait appel ici à la réflexivité de la relation qui nous assure que la classe comprend au moins un élément ayant permis de définir cette classe.

MATHINE : C'est suivant cette indication que nous allons démontrer cette proposition.

Démonstration :

En effet, si E est un ensemble, si $\mathcal{R}$ est une relation d'équivalence sur E, x un élément de E, et $\overline{x}$ sa classe d'équivalence.
Alors comme x est réflexive, $x \in \overline{x}$.
Donc $\overline{x}$ n'est pas vide.

C.Q.F.D.

Voici une nouvelle proposition, illustrant le comportement cohérent de la notion de classe d'équivalence.

Proposition **2.1.2**
Identité des classes de deux éléments de la même classe d'équivalence
Si deux éléments appartiennent à une même classe d'équivalence (cf. 2.1.5), alors leurs classes d'équivalence sont identiques.

EURISTIDE : En prenant l'exemple de la relation "est de la famille de", le sens de cette proposition, c'est que si Pierre est dans la famille que Paul, c'est-à-dire si Pierre et Paul sont en relation, donc par exemple frères, alors la famille de Pierre et égale à la famille de Paul.

MATHINE : La démonstration se fait en montrant que tout élément d'une des deux classes se trouve dans l'autre, en utilisant la transitivité de la relation d'équivalence.

Démonstration :

Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$.
Soit x et y deux éléments de E.
Supposons que $x\mathcal{R}y$.
Considérons les classes $\overline{x}$ et $\overline{y}$ de x, respectivement y.

1) Soit $z \in \overline{x}$ quelconque.
   Alors $z\mathcal{R}x$.
   Or $x\mathcal{R}y$.
   Donc $z\mathcal{R}y$ par transitivité.
   Par conséquent, $z \in \overline{y}$.
   Et donc $\overline{x} \subseteq \overline{y}$.
2) Inversement, soit $z \in \overline{y}$ quelconque.
   Alors $z\mathcal{R}y$.
   Or $x\mathcal{R}y$, donc $y\mathcal{R}x$ par symétrie.
   Donc $z\mathcal{R}x$.
   Par conséquent, $z \in \overline{x}$.
   Et donc $\overline{y} \subseteq \overline{x}$.
3) En conclusion, $\overline{x} = \overline{y}$.

C.Q.F.D.

BEATRIX : Je retiens la technique pour démontrer que deux ensembles sont égaux : il faut montrer l'inclusion dans chacun des deux sens.

EURISTIDE : Oui, c'est une technique que nous utiliserons abondamment.

MATHINE : Pour présenter la prochaine proposition, très importante, nous avons besoin de définir ce qu'est une partition.

Définition **2.1.7**
Partition d'un ensemble
On dit que des sous-ensembles d'un ensemble X forment une partition de X si tout élément de X appartient à l'un et l'un seul des sous-ensembles de X.

EURISTIDE : La partition d'un ensemble est le découpage de cet ensemble en morceaux distincts, qui ne se recouvrent pas. Le schéma ci-dessous symbolise ce découpage.

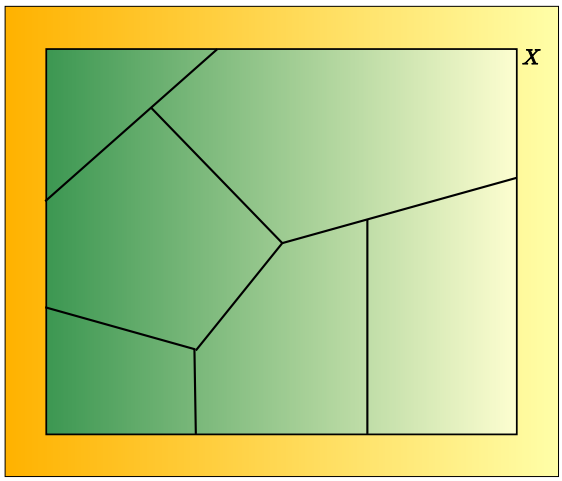

Fig. 4 - Partition d'un ensemble

Aucune des pièces n'a d'élément commun avec une autre pièce. Et l'ensemble des pièces constitue l'ensemble complet.

BEATRIX : Autrement dit, une partition est un puzzle auquel il ne manque aucune pièce !

MATHINE : Oui, c'est bien cela. Maintenant que nous avons compris la notion de partition, nous pouvons parler de la proposition fondamentale suivante.

Proposition **2.1.3**
Partition des classes d'équivalence
L'ensemble des classes d'équivalence d'un ensemble X pour une relation d'équivalence $\mathcal{R}$ constitue une partition (cf. 2.1.7) de X.

BEATRIX : Génial ! En d'autres termes, une relation d'équivalence est un générateur de puzzle sur un ensemble ?

EURISTIDE : Oui. Pour illustrer cela, reconsidérons la relation "est de la famille de". C'est par exemple le découpage des Français en familles indépendantes. Il faut noter ici que la transitivité de cette relation nous conduit à considérer la famille au sens le plus large possible ; tant qu'on trouvera des frères, soeurs, cousins, en bref des parents, de proche en proche dans la population française, il faudra les rattacher à une même famille. Nous avons donc vu ici une propriété très importante de ces relations d'équivalence, puisqu'elles divisent l'ensemble qui les porte en classes d'équivalences formant une partition. Mathine va démontrer cela immédiatement, n'est-ce pas ?

MATHINE : La démonstration se fera en trois étapes : d'abord, nous vérifierons qu'aucune classe n'est vide. Puis nous montrerons que les classes sont soit confondues, soit disjointes. Enfin, nous vérifierons que la réunion des classes forme la totalité de l'ensemble.

Démonstration :

1) Aucune classe n'est vide, d'après la proposition (2.1.1).
2) Deux classes sont disjointes ou confondues ; en effet, soit $\overline{x}$ et $\overline{y}$ deux classes.
   - Si $x\mathcal{R}y$, alors nous avons vu que $\overline{x} = \overline{y}$, d'après la proposition ((cf. 2.1.2)).
   - Si $x\neg\mathcal{R}y$, alors considérons $z \in \overline{x} \cap \overline{y}$. Alors $z \in \overline{x}$ et $z \in \overline{y}$. Donc $z\mathcal{R}x$ et $z\mathcal{R}y$, d'où $x\mathcal{R}y$, ce qui est contradictoire.
     Donc $\overline{x} \cap \overline{y} = \emptyset$.
3) La réunion des classes est X : en effet, si $x \in X$, alors $x \in \overline{x}$, donc tout élément de X appartient à une classe.

C.Q.F.D.

2.2 Scène I.2 - Ensemble quotient

EURISTIDE : L'introduction de ces relations d'équivalence et leurs classes d'équivalence vont nous permettre de construire ce qu'on appelle des ensembles quotient.

MATHINE : La structure d'ensemble quotient est encore une notion fondamentale en Algèbre.

Définition **2.2.1**
Ensemble quotient
On appelle ensemble quotient de l'ensemble X pour la relation d'équivalence (cf. 2.1.4) $\mathcal{R}$ l'ensemble des classes d'équivalence (cf. 2.1.5) de la relation $\mathcal{R}$.
Cet ensemble est noté $X/\mathcal{R}$.
A tout élément de X on peut associer sa classe d'équivalence. Ceci définit une application :

$$\begin{array}{rccc} \phi : & X & \longrightarrow & X/\mathcal{R} \\ & x & \longmapsto & \overline{x} \end{array} \tag{1}$$

EURISTIDE : La notion d'ensemble quotient est en effet essentielle en Algèbre. Je dirais qu'elle permet de ne considérer que les regroupements d'objets équivalents dans une relation d'équivalence, au lieu de considérer les objets individuels eux-mêmes. C'est donc une manoeuvre de structuration, de simplification ou encore d'abstraction : je m'intéresse aux classes ou aux familles plutôt qu'aux individus.

Le passage au quotient permet, au lieu de s'intéresser aux individus, de regarder leur classe ou groupe de rattachement. Ainsi, à l'instar de Monsieur Jourdain, nous effectuons des passages au quotient toute la journée sans le savoir, sans en avoir conscience : un zoologue, au lieu de considérer chaque félin particulier dans son individualité, va s'intéresser à la classe des lions, à la classe des tigres, des panthères, etc. Chaque regroupement des individus de cette façon est une classe d'équivalence scindant le monde des félins en autant de classes d'équivalence. Par exemple, un botaniste va souvent s'intéresser aux Rosacées, aux Composées, aux Ombelliformes, afin de mieux classer et retenir les similitudes entre les différentes espèces, plutôt que de s'intéresser, sans connaître ces classes ou familles, à chaque plante ou espèce individuellement. La classification est un moyen de simplifier, mais aussi un moyen de comprendre ou de structurer.
L'application ϕ est donc une opération d'abstraction sémantique, nous faisant passer d'un individu à sa classe d'appartenance.

BEATRIX : C'est très clair. Relation d'équivalence égale regroupement des individus en classes. Passage au quotient égale abstraction nous faisant passer du monde des individus au monde de leurs classes d'appartenance. C'est vrai que cette démarche est omniprésente dans notre vie quotidienne.

3 Acte II - Ensembles ordonnés

3.1 Scène II.1 - Ensembles ordonnés

EURISTIDE : Nous allons à présent passer aux relations d'ordre.

MATHINE : Commençons par un nouveau type de relations : les relations antisymétriques.

Définition **3.1.1**
Relation antisymétrique
Une relation $\mathcal{R}$ sur un ensemble X est dite antisymétrique si pour tout x et y appartenant à X, si $x\mathcal{R}y$ et $y\mathcal{R}x$, alors $x = y$.

EURISTIDE : La relation antisymétrique interdit un retour des flèches de relation.

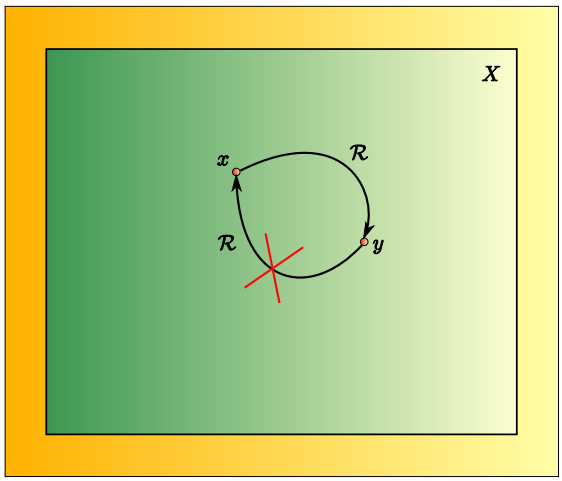

Fig. 5 - Relation antisymétrique

C'est une relation qui vise donc à ranger les objets, en mettant d'un côté ce qui est source des flèches de relation et de l'autre côté ce qui est destination des flèches de relation. Nous allons voir que ce type de relation est bien au centre de la notion de relation d'ordre.

BEATRIX : J'ai trouvé deux exemples de relations antisymétriques : "est inférieur ou égal à", "est supérieur ou égal à".

EURISTIDE : La relation "est diviseur de" est un autre exemple de relation antisymétrique dans l'ensemble des entiers naturels $\mathbb{N}$. Si a divise b et b divise a dans $\mathbb{N}$, alors nécessairement $a = b$. Ce ne serait pas vrai dans l'ensemble des entiers relatifs $\mathbb{Z}$, puisque si a divise b et b divise a dans $\mathbb{Z}$, alors $a = b$ ou $a = -b$.

MATHINE : Avec cette définition de relation antisymétrique en poche, nous allons pouvoir définir la relation d'ordre partiel.

Définition **3.1.2**
Ordre partiel
Soit E un ensemble. Un ordre partiel sur E est donné par une relation $\mathcal{R}$ réflexive (cf. 2.1.1), antisymétrique (cf. 3.1.1) et transitive (cf. 2.1.3).

BEATRIX : Pourquoi dit-on que l'ordre est "partiel" ?

EURISTIDE : Les contraintes appliquées par la définition de l'ordre, telle qu'elle est donnée ici par Mathine, n'imposent pas que tous les éléments de E soit deux à deux en relation entre eux. Il est donc possible qu'il existe des éléments qui ne soient pas ordonnés.
La relation d'ordre partiel permet de "ranger" des objets d'un ensemble. Ou, plus précisément, elle permet de ranger les objets qui sont en relation les uns avec les autres. C'est l'antisymétrie qui permet de faire concrètement ce rangement. La transitivité, quant à elle, exprime la propagation de ce rangement de proche en proche, afin que la notion de rangement ait un sens cohérent pour l'intuition.

BEATRIX : Oui, je comprends bien : par exemple, la relation "est plus grand que" permet de dire qu'un objet plus grand qu'un autre objet, lui-même plus grand qu'un troisième, est à son tour plus grand que le troisième. Si Pierre est plus agé que Paul, et si Paul est plus agé que Jacques, alors Pierre est plus agé que Jacques.

MATHINE : Nous avons parlé, à juste titre, du fait que les éléments n'étaient pas tous nécessairement en relation deux à deux. Ceci nous donne l'opportunité de définir les éléments comparables.

Définition **3.1.3**
Eléments comparables
Soit E un ensemble muni d'un ordre partiel (cf. 3.1.2) $\mathcal{R}$. On dit que des éléments x et y de E sont comparables si l'une des deux affirmations $x\mathcal{R}y$ ou $y\mathcal{R}x$ est vraie.

EURISTIDE : La notion d'éléments comparables reflète bien ce que nous voulons dire lorsque nous parlons d'ordre partiel. La relation d'ordre partiel permet de ranger les éléments, sans toutefois garantir que tous les éléments de l'ensemble E seront "rangeables". Béatrix, dans les exemples que nous avons cités tout à l'heure, il y a une bonne illustration de cela, n'est-ce pas ?

BEATRIX : Voyons, voyons : "est supérieur ou égal", non... "est inférieur ou égal", non... Je ne vois pas... Ah oui, la relation "est diviseur de" dans $\mathbb{N}$ est bien une relation d'ordre partiel. Elle permet de mettre en relation 2 et 4 par exemple, mais elle ne permet pas de mettre en relation par exemple 2 et 3. Seuls certains entiers sont en relation entre eux.

EURISTIDE : Oui, parfait. Et l'ordre partiel permet de constituer des sortes de chaînes d'éléments qui sont en relation les uns avec les autres, comme illustré ci-dessous.

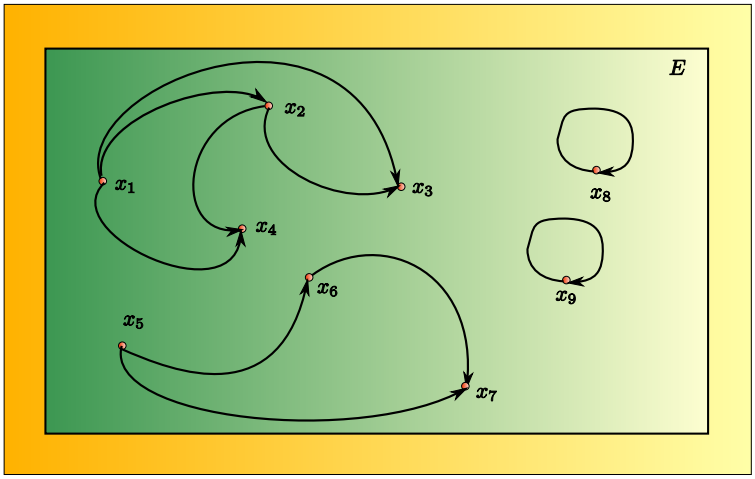

Fig. 6 - Ordre partiel

Il faut noter que puisqu'une relation d'ordre partiel est réflexive, tous les éléments sont en relation au moins avec eux-mêmes. Le fait que la relation soit "partielle"' ne signifie pas que des éléments sont en relation avec aucun élément, mais signifie qu'il existe des couples d'éléments distincts qui ne sont pas nécessairement en relation entre eux. Comme par exemple dans le schéma ci-dessus, x_8 et x_9 ou x_3 et x_4, et de nombreux autres couples.

MATHINE : Ceci nous permet d'introduire le concept d'ensemble partiellement ordonné.

Définition **3.1.4**
Ensemble partiellement ordonné
On dit qu'un ensemble est partiellement ordonné s'il existe une relation sur cet ensemble y définissant un ordre partiel (cf. 3.1.2).

EURISTIDE : Par exemple, l'ensemble des entiers naturels est partiellement ordonné par la relation "est diviseur de".

BEATRIX : Oui, puisque, comme je l'ai dit tout à l'heure, seuls certains entiers naturels sont en relation par cette relation.

MATHINE : Voyons ce qui se passe avec des sous-ensembles.

Définition **3.1.5**
Ordre partiel induit

Soit E un ensemble partiellement ordonné (cf. 3.1.4). Soit F une partie de E. F est alors aussi partiellement ordonné au moyen de l'ordre défini sur E. On dit que F est partiellement ordonné pour l'ordre partiel induit de F.

EURISTIDE : Cette définition nous explique que nous pouvons restreindre une relation d'ordre à un sous-ensemble et conserver la structure définie sur l'ensemble complet.
Ainsi, si nous prenons l'exemple de l'ensemble $\mathbb{N}$ des entiers naturels, partiellement ordonné au moyen de la relation "est diviseur de", on peut considérer le sous-ensemble F des entiers pairs, également partiellement ordonné pour l'ordre partiel induit "est diviseur de".

BEATRIX : Par exemple, dans $\mathbb{N}$, 4 divise 8. Et dans l'ensemble des entiers pairs, 4 divise 8 également. Mais dans $\mathbb{N}$, 3 divise 6. Et dans l'ensemble des entiers pairs, cette relation n'existe pas, puisque l'entier 3 ne se trouve pas dans le sous-ensemble des entiers pairs.

EURISTIDE : Nous allons maintenant voir quelques définitions et propriétés relatives au comportement des relations d'ordres aux extrémités des chaînes que nous avons vues tout à l'heure. A moins que cela soit précisé différement, nous noterons la relation d'ordre par le symbole $\leq$ dorénavant, même s'il ne s'agit pas à proprement parler de la relation "est inférieur ou égal".

MATHINE : Commençons par définir un minimum et un maximum.

Définition 3.1.6
Minimum, maximum
Soit E un ensemble partiellement ordonné (cf. 3.1.4) pour la relation $\leq$.
Un minimum de E ou un plus petit élément de E est un élément a de E tel que $\forall x \in E; a \leq x$.
Un maximum de E ou un plus grand élément de E est un élément a de E tel que $\forall x \in E; x \leq a$.

EURISTIDE : Avec cette définition, on voit qu'un plus petit élément ou plus grand élément, s'il existe, est unique. En effet, s'il existe deux plus petits éléments, par exemple, a et b, alors pour tout $x \in E$, nous avons :

$$\begin{cases} a \leq x \\ b \leq x \end{cases}. \tag{2}$$

Donc, en particulier, en choissant $x = a$, puis $x = b$:

$$\begin{cases} a \leq b \\ b \leq a. \end{cases}. \tag{3}$$

BEATRIX : Donc, par antisymétrie de la relation d'ordre, $a = b$.

EURISTIDE : Exact, Béatrix. Mais le plus petit élément ou le plus grand élément n'existent pas toujours dans une relation d'ordre partiel. Dans l'ensemble des entiers naturels, muni de la relation d'ordre partiel "est diviseur de", nous savons que 1 est diviseur de tout entier, donc 1 est le plus petit élément.

En revanche, il n'existe pas d'entier ayant pour diviseurs tous les entiers naturels. Donc il n'existe pas de plus grand élément pour cet ensemble et cette relation.

MATHINE : Présentons maintenant ce que sont l'élément maximal et l'élément minimal.

Définition **3.1.7**
Elément maximal, élément minimal
Soit E un ensemble partiellement ordonné (cf. 3.1.4) pour la relation $\leq$.
Un élément b de E est dit élément maximal s'il vérifie $\exists x \in E; b \leq x \Rightarrow x = b$.
Un élément a de E est dit élément minimal s'il vérifie $\exists x \in E; x \leq a \Rightarrow x = a$.

EURISTIDE : Un élément maximal est en quelque sorte un élément qui ne possède pas d'autre élément supérieur ou égal à lui-même, que lui-même. Ce qui ne veut pas dire qu'il est inférieur ou égal à tous les autres éléments.

BEATRIX : Oui, parce que l'ordre est partiel...

EURISTIDE : De façon similaire, un élément minimal est un élément qui ne possède pas d'autre élément inférieur ou égal à lui, que lui-même.
Un ensemble muni d'une relation d'ordre partiel ne comporte pas toujours un élément maximal ou un élément minimal. Considérons l'ensemble des entiers naturels, muni de la relation "est diviseur par". A ton avis, Béatrix, cet ensemble comporte-t-il un élément maximal ?

BEATRIX : Un élément maximal serait un entier qui n'aurait pas d'autre élément qu'il divise que lui-même, autrement dit, qui n'aurait pas d'autre multiple que lui-même. Je ne vois pas : pour un entier donné, je crois bien qu'on peut toujours lui trouver un multiple.

EURISTIDE : Tu oublies 0. Tous les multiples de 0 sont 0. Donc 0 est bien un élément maximal.
Considérons maintenant l'ensemble des entiers naturels différents de 1. Dis-moi, Béatrix, quels sont les éléments minimaux de cet ensemble muni de la relation "est diviseur de" ?

BEATRIX : Un élément minimal serait un entier qui ne serait divisible que par lui-même. Comme nous avons ôté 1 de l'ensemble, on peut dire que les nombres premiers sont des éléments minimaux.

MATHINE : Bravo ! Voyons maintenant ce qu'est un ensemble ordonné où tous les éléments sont en relation entre eux deux à deux.

Définition **3.1.8**
Ensemble totalement ordonné
Soit E ensemble partiellement ordonné (cf. 3.1.4) pour la relation $\leq$. Si pour tout x et y appartenant à E, une et une seule des deux relations $x \leq y$ et $y \leq x$ est vraie dans E, alors E est dit totalement ordonné .

EURISTIDE : Nous avons vu que l'ensemble des entiers muni de la relation "est diviseur de" n'est pas totalement ordonné, puisque certains entiers ne sont pas diviseurs d'autres entiers.
En revanche, l'ensemble des entiers muni de la relation "est inférieur ou égal à" est bien un ensemble totalement ordonné, car tous les entiers naturels sont alors en relation entre eux.

MATHINE : Voyons les minorant et majorant maintenant.

Définition 3.1.9
Minorant, majorant
Soit E un ensemble partiellement ordonné (cf. 3.1.4) pour la relation $\leq$. Soit F une partie de E.
Un élément a de E est un minorant de F si $\forall x \in F; a \leq x$.
Un élément b de E est un majorant de F si $\forall x \in F; x \leq b$.

EURISTIDE : Il faut bien noter ici que le minorant ou le majorant peut être élément du sous-ensemble F, mais ce n'est pas toujours le cas ; il peut se trouver en dehors de F. Par exemple, le schéma suivant illustre le fait que a est un minorant de F.

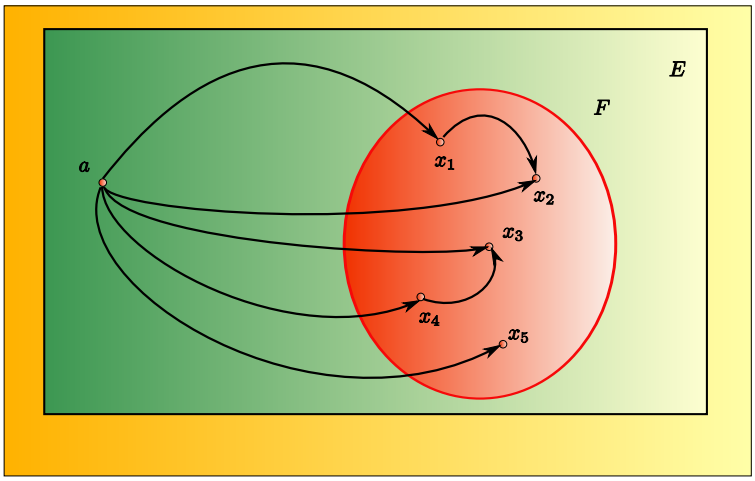

Fig. 7 - Minorant externe au sous-ensemble

Par exemple, pour la relation "est diviseur de", 2 est un minorant du sous-ensemble F des entiers pairs dans l'ensemble des entiers naturels $\mathbb{N}$. 2 appartient à F. Mais, par exemple, 1 est également un minorant de l'ensemble F, et A n'appartient pas à F.
Considérons le sous-ensemble F des chiffres de 0 à 9 dans l'ensemble des entiers naturels $\mathbb{N}$. Munissons ces

ensembles de la relation "est inférieur ou égal". Alors 9 est un majorant de F. Mais 10 est également un majorant de F, qui n'appartient pas à F.

MATHINE : Nous allons finir ce panorama des éléments particuliers d'une relation d'ordre par les bornes inférieure et supérieure.

Définition **3.1.10**
Borne inférieure, borne supérieure
Soit E un ensemble partiellement ordonné. Soit F une partie de E.
Un élément a de E est une borne inférieure de F si c'est le plus grand des minorants (cf. 3.1.9) de F. Autrement dit, a est un minorant (cf. 3.1.9) de F et si x est un minorant de F, alors $x \leq a$.
Un élément b de E est une borne supérieure de F si c'est le plus petit des majorants (cf. 3.1.9) de F. Autrement dit, b est un majorant (cf. 3.1.9) de F et si x est un majorant de F, alors $b \leq x$.

EURISTIDE : En reprenant l'exemple précédent du sous-ensemble F des entiers pairs muni dans l'ensemble des entiers naturels de la relation "est diviseur de", on voit que 2 est bien une borne inférieure de F, car c'est le plus grand des minorants de F. En revanche, 1 est bien un minorant, mais n'est pas une borne inférieure.

BEATRIX : Je vais essayer de récapituler ce que nous avons vu concernant ces éléments particuliers des relations d'ordre. Je vais parler uniquement des éléments "en bas de l'échelle"' pour illustrer ce que je dis. Le plus petit élément est celui qui est inférieur ou égal à tous les autres. L'élément minimal est celui qui n'a pas d'autre élément plus petit que lui-même. Le minorant d'un sous-ensemble F est un élément de E plus petit que tous les éléments de F. Il n'est pas nécessairement dans F. Et enfin, la borne inférieure est le plus grand des minorants. Il n'est pas non plus nécessairement dans F.

EURISTIDE : C'est un bon résumé de cette forme des relations d'ordre.
Nous allons terminer cette partie en abordant l'important Lemme de Zorn ou Axiome du choix.

BEATRIX : Hum, hum... C'est un titre bien mystérieux.

3.2 Scène II.2 - Lemme de Zorn

MATHINE : Commençons par quelques définitions nécessaires.

Définition **3.2.1**
Ensemble inductif
Soit E un ensemble totalement ordonné. E est dit inductif si toute partie de E non vide et totalement ordonnée (cf. 3.1.8) possède un majorant (cf. 3.1.9).

EURISTIDE : Prenons l'exemple de l'ensemble des entiers inférieurs ou égaux à 99, muni de la relation "est inférieur ou égal". C'est bien un ensemble inductif, puisque toute partie de cet ensemble possède

un majorant.
En revanche, l'ensemble des entiers naturels dans sa totalité n'est pas inductif. Bien qu'il soit totalement ordonné, ses parties ne possèdent pas, si elles sont infinies, de majorant.

BEATRIX : Pourquoi a-t-on choisi ce terme d'inductif ?

EURISTIDE : Le terme "inductif suggère que l'on peut induire, à partir de toute partie totalement ordonnée, un majorant.

MATHINE : Nous allons voir tout de suite, avec la notion de chaîne et de maillon, que ce terme prend tout son sens.

Définition **3.2.2**
Chaîne et maillons
Soit E un ensemble partiellement ordonné (cf. 3.1.4). Une partie de E totalement ordonnée (cf. 3.1.8) est appelée une chaîne . Un élément d'une chaîne est appelé un maillon .

EURISTIDE : L'idée de chaîne au sein d'un ensemble partiellement ordonné permet d'imager une suite d'éléments en relation et donc rangés les uns par rapport aux autres.

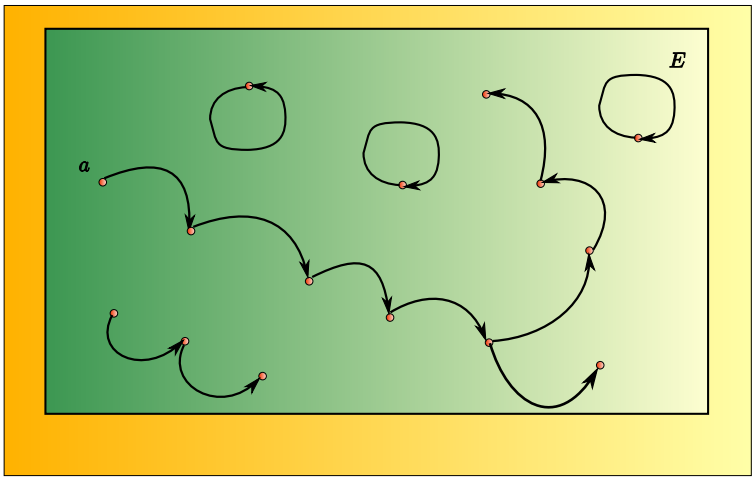

Fig. 8 - Chaînes et maillons

Je n'ai pas représenté ici les relations résultant de la transitivité de la relation d'ordre, pour plus de clarté dans le schéma. L'extrémité de chaque chaîne constitue l'induction dont nous parlions précédemment. Un ensemble inductif est donc tel que toute chaîne conduit à au moins un majorant.

MATHINE : Voyons maintenant la définition d'un ensemble strictement inductif.

Définition **3.2.3**
Ensemble strictement inductif
Un ensemble E partiellement ordonné (cf. 3.1.4) est dit strictement inductif si toute partie non vide de E possède une borne supérieure (cf. 3.1.10).

BEATRIX : Il s'agit d'un perfectionnement supplémentaire de l'ensemble inductif.

EURISTIDE : Oui. Il faut comprendre la notion d'ensemble strictement inductif comme étant un ensemble où l'on peut toujours déduire d'une partie non vide une borne supérieure, c'est-à-dire un plus petit majorant, à l'extrémité d'une chaîne.

MATHINE : Et voici enfin le fameux Lemme de Zorn.

Définition **3.2.4**
Lemme de Zorn
Tout ensemble ordonné (cf. 3.1.8) non vide et inductif (cf. 3.2.1) possède un élément maximal (cf. 3.1.7).

EURISTIDE : Ce lemme, appelé également axiome du choix, permet de choisir dans un ensemble inductif un élément maximal. C'est donc la possibilité de choisir, sur un critère donné par la relation d'ordre, un élément particulier qui est supérieur à au moins un élément de cet ensemble.
Par exemple, si je considère l'ensemble des entiers inférieurs ou égaux à 99, muni de la relation "est inférieur ou égal", on peut toujours choisir un entier qui est supérieur ou égal à tous les éléments d'un sous-ensemble de cet ensemble.

BEATRIX : Ceci justifie bien le nom d'axiome du choix. Il veut dire qu'on peut choisir des éléments dans un ensemble inductif.

4 Acte III - Groupes

4.1 Scène III.1 - Vocabulaire

EURISTIDE : Nous voici arrivés au chapitre des groupes. Nous verrons l'importance de cette structure de groupe tout au long de nos discussions sur l'Algèbre et tous les développements qui fondent et découlent de la théorie des nombres moderne.

BEATRIX : Si je comprends bien, c'est une discussion importante que nous allons avoir ici.

EURISTIDE : Oui, encore plus importante que les autres.

MATHINE : Nous allons, comme d'habitude, débuter par une série de définitions pour introduire la structure de groupe. Commençons par définir la loi interne d'un groupe.

Définition **4.1.1**
Loi interne
On appelle loi interne sur G une application $G \times G \longrightarrow G$.

EURISTIDE : Il s'agit donc d'une loi transformant deux éléments de G ou un élément de G. Le qualificatif d'interne nous indique que la loi opère à l'intérieur de l'ensemble G. On dit aussi que G est stable pour cette loi.
Des exemples de lois internes sur l'ensemble des entiers sont l'addition et la multiplication.

BEATRIX : Ce sont même les bases de l'arithmétique que nous apprenons à l'école primaire...

MATHINE : Voyons la propriété d'associativité d'une loi interne.

Définition **4.1.2**
Loi associative
Soit $\perp$ une loi interne (cf. 4.1.1) sur G. Une loi est dite associative si pour tout x, y, z dans G, $(x \perp y) \perp z = x \perp (y \perp z)$.

EURISTIDE : La notion d'associativité permet de grouper les éléments mis en relation par la loi. C'est une propriété très naturelle lorsque nous pensons à l'addition par exemple :

$$2 + (4 + 8) = 2 + 12 = 14 \quad (4)$$
$$(2 + 4) + 8 = 6 + 8 = 14. \quad (5)$$

Mais, ceci est moins évident quand nous prenons pour loi interne la division, par exemple :

$$(8/4)/2 = 1 \quad (6)$$
$$8/(4/2) = 4. \quad (7)$$

Donc :

$$(8/4)/2 \neq 8/(4/2). \quad (8)$$

La division n'est donc pas une loi associative.

MATHINE : Voyons maintenant la notion d'élément neutre.

Définition **4.1.3**
Elément neutre
Soit $\perp$ une loi interne (cf. 4.1.1) sur G. On appelle élément neutre un élément e de G tel que pour tout x appartenant à G, $x \perp e = e \perp x = x$.

BEATRIX : Pour l'addition dans $\mathbb{N}$, l'élément neutre est 0, puisque :

$$\forall x \in \mathbb{N}, \quad x + 0 = 0 + x = x. \tag{9}$$

EURISTIDE : Tout à fait. Et pour la multiplication dans $\mathbb{N}$, l'élément neutre est 1, puisque $\forall x \in \mathbb{N}, x \times 1 = 1 \times x = x$. On peut imaginer des lois n'ayant pas d'élément neutre. Par exemple, imaginons la loi $\oplus$ dans $\mathbb{N}$ qui associe à deux entiers a et b :

$$a \oplus b = a + b + 1. \tag{10}$$

C'est bien une loi interne dans $\mathbb{N}$.
Elle est associative car :

$$\begin{aligned}
(a \oplus b) \oplus c &= (a + b + 1) \oplus c && (11)\\
&= (a + b + 1) + c + 1 && (12)\\
&= a + (b + c + 1) + 1 && (13)\\
&= a + (b \oplus c) + 1 && (14)\\
&= a \oplus (b \oplus c). && (15)
\end{aligned}$$

Mais elle ne possède pas d'élément neutre dans $\mathbb{N}$.

BEATRIX : C'est vrai. Mais si on considérait la même loi dans l'ensemble des entiers relatifs $\mathbb{Z}$, nous pourrions lui trouver un élément neutre : -1, car :

$$\begin{aligned}
a \oplus -1 &= a + (-1) + 1 && (16)\\
&= a && (17)\\
-1 \oplus a &= -1 + a + 1 && (18)\\
&= a. && (19)
\end{aligned}$$

MATHINE : Regardons maintenant ce qu'est l'inverse d'un élément.

Définition **4.1.4**
Inverse
Soit $\perp$ une loi interne (cf. 4.1.1) sur G. Soit x un élément de G. Supposons que la loi $\perp$ admette un élément neutre (cf. 4.1.3) e dans G. On appelle inverse de x un élément y de G tel que $x \perp y = y \perp x = e$. Cet inverse est en général noté x^{-1}.

EURISTIDE : Dans le cas de la loi d'addition dans l'ensemble des entiers relatifs, l'inverse d'un élément de a est bien connu et est appelé l'opposé de a et noté $-a$.
Pour les éléments réels non nuls, l'inverse d'un élément de x est appelé justement inverse, et noté $\frac{1}{x}$.
L'inverse n'existe pas toujours. Par exemple pour l'ensemble des entiers naturels non nuls, muni de la loi de multiplication, seul 1 possède un inverse.

MATHINE : Ayant parcouru les définitions de base, nous pouvons maintenant construire la structure de groupe.

Définition **4.1.5**
Groupe
On dit qu'un ensemble G, muni d'une loi (cf. 4.1.1) $\perp$ possède une structure de groupe si :
- *$\perp$ est associative (cf. 4.1.2) ;*
- *Il existe un élément neutre (cf. 4.1.3) e pour $\perp$ dans G ;*
- *Tout élément de G possède un inverse (cf. 4.1.4) dans G pour $\perp$.*

On note $(G, \perp)$ le groupe G muni de la loi $\perp$.

EURISTIDE : La structure de groupe permet de formaliser un certain type de symétrie dans un ensemble. Existence d'un inverse, capacité à utiliser les parenthèses dans les calculs (associativité).
La structure de groupe est la structure privilégiée des opérations géométriques telles que les rotations ou les opérations de transformations linéaires que nous verrons plus tard.
Quoi qu'il en soit, chaque fois que vous avez affaire à une structure où un élément peut être neutre, et où des éléments peuvent s'annuler (rotation et rotation inverse, transformation géométrique et transformation inverse, addition et opposé), vous pouvez suspecter la présence d'une structure de groupe.

BEATRIX : Je vois un exemple évident, c'est l'ensemble $\mathbb{Z}$ muni de l'addition. L'élément neutre est 0. L'inverse d'un élément a est l'élément $-a$.

EURISTIDE : Oui, c'est un premier exemple banal.
Un autre exemple, plus complexe, est l'ensemble des manipulations du Rubik's cube, muni de la loi de composition des manipulations. Une manipulation est une succession de rotations de base des faces du cube. La loi de composition des manipulations est associative ; elle a pour élément neutre l'absence de rotation. L'inverse d'une manipulation est la manoeuvre inverse consistant à effectuer les rotations composant la manipulation d'origine dans l'ordre inverse et dans le sens inverse.

BEATRIX : C'est amusant de penser que le célèbre Rubik's cube donne le jour à une structure de groupe !

EURISTIDE : Oui. Et il y a d'ailleurs des ouvrages très sérieux qui décrivent et analysent la structure de groupe du Rubik's cube. Cela permet, entre autres, de calculer le nombre de positions possibles du cube, et de déterminer les algorithmes de résolution.

BEATRIX : Extraordinaire ! Résoudre le Rubik's cube par des calculs, par la seule force de la pensée et de la structure de groupe...

MATHINE : Nous allons voir maintenant notre première proposition concernant les groupes. Il s'agit de démontrer que l'élément neutre et l'inverse d'un élément dont nous avons parlé à propos d'un groupe sont uniques.

Proposition 4.1.1
Unicité élément neutre et inverse
Soit G un groupe (cf. 4.1.5) pour la loi $\perp$ et soit e un élément neutre (cf. 4.1.3) de G. Alors :

1. *L'élément neutre de G est unique ;*
2. *$e^{-1} = e$;*
3. *Tout élément x de G possède un inverse (cf. 4.1.4) unique*

EURISTIDE : Ces propriétés découlent de façon assez évidente des définitions. Béatrix, peux-tu essayer ? Il suffit de faire des démonstrations par l'absurde.

BEATRIX : Oui, je vais me lancer.

Démonstration :

1) Supposons qu'il existe deux éléments neutres e et e'.
Par définition, pour tout $x \in G$:

$$x \perp e = x, \tag{20}$$

et :

$$x \perp e' = x. \tag{21}$$

Donc :

$$x \perp e = x \perp e'. \tag{22}$$

Nous pouvons multiplier les deux membres de l'égalité ci-dessus par l'inverse de x :

$$x^{-1} \perp (x \perp e) = x^{-1} \perp (x \perp e'). \tag{23}$$

En utilisant l'associativité :

$$(x^{-1} \perp x) \perp e = (x^{-1} \perp x) e'. \tag{24}$$

D'où :

$$e \perp e = e \perp e', \tag{25}$$

et donc enfin :

$$e = e'. \tag{26}$$

Donc, l'élément neutre est unique.

2) e^{-1} est par définition tel que :

$$e^{-1} \perp e = e. \tag{27}$$

Or, par définition de e,

$$e^{-1} \perp e = e^{-1}. \tag{28}$$

D'où :

$$e^{-1} = e. \tag{29}$$

3) Soit x un élément de G.
Supposons que x ait deux inverses y et y'.
Alors, par définition :

$$x \perp y = e, \tag{30}$$

et :

$$x \perp y' = e. \tag{31}$$

Donc :

$$x \perp y = x \perp y'. \tag{32}$$

En multipliant à gauche les deux membres de l'égalité par x^{-1}, on obtient :

$$x^{-1} \perp (x \perp y) = x^{-1} \perp (x \perp y'). \tag{33}$$

D'où :

$$(x^{-1} \perp x) \perp y = (x^{-1} \perp x) \perp y', \tag{34}$$

et par conséquent :

$$e \perp y = e \perp y'. \tag{35}$$

D'où :

$$y = y'. \tag{36}$$

C.Q.F.D.

EURISTIDE : Bravo Béatrix, pour cette démonstration rondement menée. L'unicité de l'élément neutre nous permet en particulier de chercher cet élément neutre à tatons ou par essais successifs, et d'être certains d'avoir "le bon" une fois qu'il en est trouvé un.

MATHINE : Voyons maintenant en outre le concept de loi interne commutative.

Définition **4.1.6**
Loi commutative
Une loi (cf. 4.1.1) $\perp$ sur G est dite commutative si pour tout x, y appartenant à G, on a $x \perp y = y \perp x$.

EURISTIDE : L'exemple classique, sur l'ensemble des entiers relatifs, de loi commutative, est l'addition.

BEATRIX : Ou la multiplication.

EURISTIDE : En revanche, sur $\mathbb{Z}$, la soustraction n'est pas commutative. A priori :

$$a - b \neq b - a. \tag{37}$$

Par exemple :

$$1 = 3 - 2 \neq 2 - 3 = -1. \tag{38}$$

BEATRIX : Et sur l'ensemble des entiers rationnels $\mathbb{Q}$, la division n'est pas commutative non plus :

$$\frac{a}{b} / \frac{c}{d} = \frac{ad}{bc}, \tag{39}$$

et :

$$\frac{c}{d} / \frac{a}{b} = \frac{cd}{da}. \tag{40}$$

Donc, a priori :

$$\frac{a}{b} / \frac{c}{d} \neq \frac{c}{d} / \frac{a}{b}. \tag{41}$$

Par exemple :

$$\frac{2}{3} = \frac{\frac{1}{2}}{\frac{3}{4}} \neq \frac{\frac{3}{4}}{\frac{1}{2}} = \frac{3}{2}. \tag{42}$$

MATHINE : Et cette définition de la commutativité nous permet de définir les groupes abéliens.

Définition **4.1.7**
Groupe abélien
On dit que le groupe $(G, \perp)$ est abélien si la loi $\perp$ est commutative (cf. 4.1.6).

BEATRIX : Un exemple évident de groupe abélien est l'ensemble des entiers relatifs $\mathbb{Z}$ muni de la loi d'addition.
Avez-vous un exemple de groupe non abélien ?

EURISTIDE : Un exemple de groupe non abélien peut être donné par l'ensemble des matrices carrées 2×2, à coefficients réels, inversibles, muni de la loi de multiplication des matrices. Nous verrons plus tard la définition et les propriétés formelles de ces matrices.
Une matrice carrée 2×2 est un objet de la forme :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}, \tag{43}$$

où $a, b, c, d \in \mathbb{R}$.
La loi de multiplication $\otimes$ de ces matrices carrées est définie par :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \otimes \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \begin{pmatrix} aa' + cb' & ac' + cd' \\ ba' + bb' & bc' + dd' \end{pmatrix}. \tag{44}$$

Nous allons voir que cette loi n'est pas commutative, et que pourtant il s'agit bien d'un groupe.

1) Commutativité :
Nous avons :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \otimes \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \begin{pmatrix} aa' + cb' & ac' + cd' \\ ba' + bb' & bc' + dd' \end{pmatrix} \tag{45}$$

et :

$$\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} \otimes \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a'a + c'b & a'c + c'd \\ b'a + d'b & b'c + d'd \end{pmatrix}. \tag{46}$$

A priori, par exemple, dans le cas général, $aa' + cb' \neq a'a + c'b$, donc la loi $\otimes$ n'est pas commutative.

2) Associativité :

$$\left(\begin{pmatrix} a & c \\ b & d \end{pmatrix} \otimes \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} \right) \otimes \begin{pmatrix} a'' & c'' \\ b'' & d'' \end{pmatrix} = \begin{pmatrix} aa' + cb' & ac' + cd' \\ ba' + bb' & bc' + dd' \end{pmatrix} \otimes \begin{pmatrix} a'' & c'' \\ b'' & d'' \end{pmatrix} \tag{47}$$

$$= \begin{pmatrix} aa'a'' + cb'a'' + ac'b'' + cd'b'' & aa'c'' + cb'c'' + ac'd'' + cd'd'' \\ ba'a'' + bb'a'' + bc'b'' + dd'b'' & ba'c'' + bb'c'' + bc'd'' + dd'd'' \end{pmatrix} \tag{48}$$

et :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \otimes \left(\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} \otimes \begin{pmatrix} a'' & c'' \\ b'' & d'' \end{pmatrix} \right) = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \otimes \begin{pmatrix} a'a'' + c'b'' & a'c'' + c'd'' \\ b'a'' + d'b'' & b'c'' + d'd'' \end{pmatrix} \tag{49}$$

$$= \begin{pmatrix} aa'a'' + ac'b'' + cb'a'' + cd'b'' & aa'c'' + ac'd'' + cb'c'' + cd'd'' \\ ba'a'' + bc'b'' + db'a'' + dd'b'' & ba'c'' + bc'd'' + db'c'' + dd'd'' \end{pmatrix} \tag{50}$$

En ordonnant les termes de chacune des matrices par ordre croissant a, b, c, on obtient, d'une part pour la première expression :

$$\begin{pmatrix} aa'a'' + a''b'c + ab''c' + b''cd' & aa'c'' + b'cc'' + ac'd'' + cd'd'' \\ a'a''b + a''bb' + bb''c' + b''dd' & a'bc'' + bb'c'' + bc'd'' + dd'd'' \end{pmatrix} \tag{51}$$

et pour la seconde expression :

$$\begin{matrix} aa'a'' + ab''c' + a''b'c + b''cd' & aa'c'' + ac'd'' + b'cc'' + cd'd'' \\ a'a''b + bb''c' + a''b'd + b''dd' & a'bc'' + bc'd'' + b'c''d + dd'd'' \end{matrix} \tag{52}$$

Et l'on voit immédiatement que ces deux matrices sont identiques. Donc la loi est associative.

3) Elément neutre :
L'élément neutre est la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. En effet :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a+0 & 0+c \\ b+0 & 0+d \end{pmatrix} \tag{53}$$

$$= \begin{pmatrix} a & c \\ b & d \end{pmatrix} \tag{54}$$

et :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a+0 & c+0 \\ 0+b & 0+d \end{pmatrix} \tag{55}$$

$$= \begin{pmatrix} a & c \\ b & d \end{pmatrix} \tag{56}$$

4) Inverse :

L'inverse d'une matrice $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ est tel que :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \otimes \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{57}$$

Donc, tel que :

$$\begin{cases} aa' + cb' &= 1 \\ a'b + db' &= 0 \\ ac' + cd' &= 0 \\ bc' + dd' &= 1. \end{cases} \tag{58}$$

En multipliant la première équation par b, on obtient :

$$aa'b + cb'b = b, \tag{59}$$

et la deuxième par a :

$$aa'b + adb' = 0. \tag{60}$$

D'où, en soustrayant les deux équations :

$$cb'b - adb' = b. \tag{61}$$

Soit :

$$b'(cb - ad) = b. \tag{62}$$

Donc :

$$b' = \frac{b}{bc - ad}. \tag{63}$$

Ici, et pour la suite de la démonstration, on suppose que $bc - ad \neq 0$, en considérant que c'est une condition nécessaire pour que la matrice soit inversible.
Or, d'après la deuxième équation :

$$a'b = -db'. \tag{64}$$

Donc :

$$a' = \frac{-d}{bc - ad}. \tag{65}$$

De même, en multipliant la troisième équation par b, on obtient :

$$abc' + cbd' = 0, \tag{66}$$

et en multipliant la quatrième équation par a, on a :

$$abc' + add' = a. \tag{67}$$

D'où :

$$add' - cbd' = a, \tag{68}$$

ou encore :

$$d' = \frac{-a}{bc - ad}. \tag{69}$$

Or, d'après la troisième équation :

$$ac' = -cd', \tag{70}$$

d'où :

$$c' = \frac{c}{bc - ad}. \tag{71}$$

Donc, la matrice inverse, si elle existe, est :

$$\begin{pmatrix} \frac{-d}{bc-ad} & \frac{c}{bc-ad} \\ \frac{b}{bc-ad} & \frac{-a}{bc-ad} \end{pmatrix} \tag{72}$$

Puisque la loi $\otimes$ n'est pas commutative, il faut vérifier que cet inverse est valide à gauche également :

$$\begin{pmatrix} \frac{-d}{bc-ad} & \frac{c}{bc-ad} \\ \frac{b}{bc-ad} & \frac{-a}{bc-ad} \end{pmatrix} \otimes \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} \frac{-ad+bc}{bc-ad} & \frac{ac-ac}{bc-ad} \\ \frac{ab-ab}{bc-ad} & \frac{bc-ad}{bc-ad} \end{pmatrix} \tag{73}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{74}$$

Donc, cette structure est bien une structure de groupe.

4.2 Scène III.2 - Sous-groupe d'un groupe

BEATRIX : L'étude de ces matrices me semble très intéressante. A quoi ces matrices servent-elles ?

EURISTIDE : Les matrices sont très utiles à l'étude des applications linéaires. Nous verrons cela en détail lorsque Mathine nous parlera des applications linéaires.
Dans l'immédiat, nous allons revenir aux groupes et introduire la notion de sous-groupe. Les sous-groupes sont aux groupes ce que les sous-ensembles sont aux ensembles.

MATHINE : La particularité toutefois des sous-groupes, c'est que nous allons y transporter la structure du groupe.

Définition **4.2.1**
Sous-groupe
Soit H un sous ensemble de G. On dit que $(H, \perp)$ est un sous groupe de G si la restriction de la loi (cf. 4.1.1) $\perp$ de G à H définit une structure de groupe (cf. 4.1.5) sur H.

EURISTIDE : Par exemple, l'ensemble des entiers relatifs pairs est un sous-groupe de l'ensemble des entiers relatifs muni de la loi d'addition (0 étant considéré comme un élément pair).

BEATRIX : Si je comprends bien, pour obtenir un sous-groupe H à partir d'un groupe G, il faut chercher un sous-ensemble H qui contient l'élément neutre de G, et qui est stable pour la loi interne. Par exemple, l'ensemble des entiers relatifs impairs n'est pas un sous-groupe de $(\mathbb{Z}, +)$ pour deux raisons : il ne contient pas 0 qui est l'élément neutre, et de plus, la somme de deux entiers impairs n'est pas impaire.

MATHINE : Nous allons voir justement comment caractériser un sous-groupe.

Proposition **4.2.1**
Qualification d'un sous-groupe
On a équivalence entre :

- *$(H, \perp)$ est un sous-groupe (cf. 4.2.1) de G.*
- *e est un élément de H et pour tout x, y dans H, $x \perp y^{-1}$ est élément de H.*

EURISTIDE : Cette caractérisation est évidemment très utile car elle permet de diminuer l'effort de vérification quand on veut mettre en évidence l'existence d'un sous-groupe.

MATHINE : La démonstration se fait naturellement en montrant les deux sens de l'équivalence.

Démonstration :

1) Soit $(H, \perp)$ un sous-groupe de G. Démontrons les deux propriétés caractéristiques.
   a) Soit e' l'élément neutre de $(H, \perp)$.
   Par définition, pour tout $x \in H$, on a :
   $$x \perp e' = x. \tag{75}$$
   On peut considérer x comme un élément de G. Alors, nous savons que nous avons :
   $$x \perp e = x. \tag{76}$$
   Il s'ensuit que :
   $$x \perp e = x \perp e'. \tag{77}$$
   On déduit de cette égalité que $e = e'$, en multipliant, dans G, les deux membres de l'égalité par l'inverse x^{-1} de x, à gauche.
   Donc e est élément neutre de H, et par conséquent, a fortiori il appartient à H.
   b) Soit $x, y \in H$.
   Soit y' l'inverse de y dans H. Par définition :
   $$y \perp y' = e. \tag{78}$$
   Or, dans G, si nous considérons l'inverse y^{-1} de y, par définition nous avons :
   $$y \perp y^{-1} = e. \tag{79}$$
   Donc :
   $$y \perp y' = y \perp y^{-1}, \tag{80}$$
   d'où, en multipliant les deux membres de l'égalité à gauche par l'inverse de y dans G :
   $$y' = y^{-1}. \tag{81}$$
   Donc, l'inverse de y dans H est y^{-1}.
   Or H est un sous-groupe, donc il s'ensuit que le produit de deux éléments de H se trouve dans H, donc :
   $$x \perp y^{-1} \in H. \tag{82}$$
2) Supposons que H soit un sous-ensemble de G tel que $e \in H$ et $\forall x, y \in H, \quad x \perp y^{-1} \in H$. Nous allons démontrer que H est un sous-groupe de G.
   a) Comme H est un sous-ensemble du groupe G, comme tous les éléments de G respectent l'associativité, a fortiori ceux de H aussi.

b) Nous savons que $e \in H$.
Considérons $x \in H$ quelconque.
Alors $x \in G$ également. Donc :

$$x \perp e = e \perp x = x. \tag{83}$$

Donc e est élément neutre de $\perp$ dans H.

c) Considérons $e \in H$ et $y \in H$.
En appliquant la propriété :

$$\forall x, y \in H, \quad x \perp y^{-1} \in H, \tag{84}$$

aux deux éléments e et y, nous obtenons :

$$\forall y \in H, \quad e \perp y^{-1} \in H. \tag{85}$$

Ce qui s'écrit :

$$\forall y \in H, \quad y^{-1} \in H. \tag{86}$$

Or y et y^{-1} sont également dans G, donc :

$$y \perp y^{-1} = y^{-1} \perp y = e. \tag{87}$$

Donc, y^{-1} est l'inverse de y dans H.

C.Q.F.D.

BEATRIX : C'est une démonstration assez aisée. Mais je retiens qu'il ne faut a priori pas confondre l'inverse de y dans G et celui dans H, avant d'avoir démontré qu'ils sont identiques, sous peine de faire une erreur de raisonnement.

4.3 Scène III.3 - Homomorphisme de groupe

EURISTIDE : Oui, c'est ce qui fait la finesse de ce genre de démonstration qui paraît facile, au premier abord.
Nous allons maintenant pouvoir introduire le concept de morphisme, c'est-à-dire construire des applications qui transportent la structure de groupe.

BEATRIX : Je suppose que ce concept va être de nouveau essentiel pour nos discussions futures. Je sens tout de suite que le transport de structure est quelque chose de très important et permettra également de construire des structures sur de nouveaux ensembles, n'est-ce pas ?

EURISTIDE : En effet, les morphismes constituent un outil très puissant en Algèbre, puisqu'ils aident le mathématicien à transporter ou copier des structures d'un ensemble sur un autre. Le morphisme, c'est un peu la photocopieuse de structures ; c'est donc l'outil quotidien de l'algébriste. On parle aussi d'homomorphisme, à la place du mot morphisme.

MATHINE : Commençons par en formaliser la définition.

Définition **4.3.1**
Homomorphisme de groupe
Soit $(G, \perp)$ et $(H, \top)$ des groupes (cf. 4.1.5). On dit qu'une application $f : G \longrightarrow H$ est un homomorphisme de groupe si :
- *$f(e_G) = e_H$;*
- *Si x et y sont éléments de G, $f(x \perp y) = f(x) \top f(y)$.*

EURISTIDE : Comme je l'ai dit, cette notion est essentielle. Fondamentalement, elle permet de lier deux groupes au moyen de la fonction f, et en assurant que la fonction transporte en quelque sorte, de façon cohérente, la loi interne de G vers la loi interne de H. C'est donc qu'elle va nous permettre de transporter une structure de groupe d'un ensemble sur un autre, en définissant la loi de la seconde structure $\top$ au moyen de la relation suivante :

$$f(x) \top f(y) = f(x \perp y), \tag{88}$$

ceci à condition que tout élément de H ait effectivement un antécédent par f dans G. Nous verrons plus loin qu'une telle application est dite surjective.

BEATRIX : Avez-vous un exemple ?

EURISTIDE : Un exemple typique d'homomorphisme de groupes peut être construit en considérant d'une part l'ensemble des entiers relatifs muni de la loi d'addition, et d'autre part l'ensemble des entiers relatifs pairs (0 compris) muni de la loi d'addition. L'application qui associe à un entier son double est un homomorphisme de groupes car :

$$2 \times 0 = 0 \tag{89}$$
$$2(x + y) = 2x + 2y. \tag{90}$$

MATHINE : Continuons avec le cas particulier où les deux sous-groupes sont identiques.

Définition **4.3.2**
Endomorphisme de groupe
Soit $(G, \perp)$ un groupe (cf. 4.1.5). On dit qu'une application $f : G \longrightarrow G$ est un endomorphisme de groupe si f est un homomorphisme (cf. 4.3.1) de G dans G.

EURISTIDE : Les endomorphismes de groupe ont un rôle un peu différent. Ce sont des applications qu'on peut considérer comme compatibles avec la loi de groupe. Autrement dit, elles conservent cette loi et donc la structure de groupe. Ce n'est pas le cas de toutes les applications sur un groupe.
Par exemple, dans l'ensemble des entiers relatifs, l'application $x \mapsto x + 1$ n'est pas un endomorphisme, car elle ne conserve pas l'élément neutre. En revanche, l'application $x \mapsto 2x$ est bien un endomorphisme sur ce même groupe.

BEATRIX : J'ai tout de même une remarque. L'endomorphisme $x \mapsto 2x$ parcourt bien tout le groupe $(\mathbb{Z}, +)$. Mais les images de l'endomorphisme ne parcourent pas la totalité de $\mathbb{Z}$: elles sont confinées aux

éléments pairs. C'est donc un homomorphisme qui, à proprement parler, ne s'applique que de $\mathbb{Z}$ sur son sous-groupe $2\mathbb{Z}$.

EURISTIDE : C'est vrai. Cependant, on continue de dire que $x \mapsto 2x$ est un endomorphisme de $\mathbb{Z}$, et nous allons introduire la nuance dont tu parles en distinguant les applications injectives des autres applications.

MATHINE : Nous allons donc commencer par définir ce qu'est l'injectivité.

Définition **4.3.3**
Application injective
On dit qu'une application f d'un ensemble G dans un ensemble H est injective si pour tout x, y appartenant à G, $f(x) = f(y) \Rightarrow x = y$.

EURISTIDE : Cette propriété d'une application nous permet, ainsi que la suivante, de qualifier la façon dont les applications transforment les ensembles sur lesquels elles s'appliquent.
Une application injective n'autorise pas que deux éléments différents aient une image commune. Autrement dit, elles interdisent le schéma suivant.

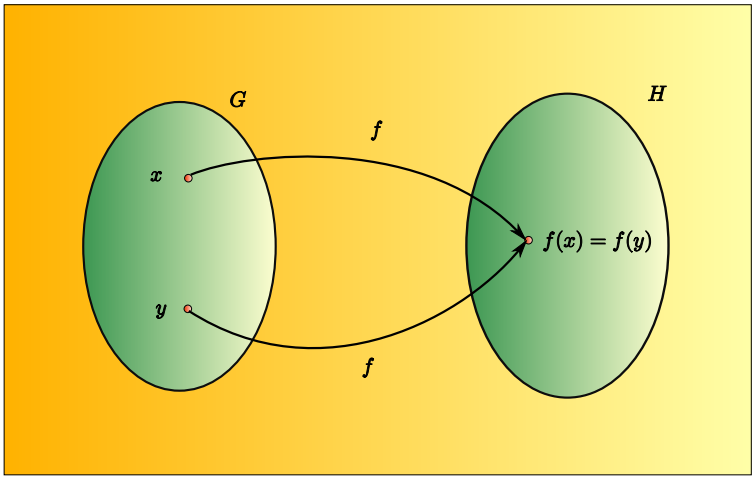

Fig. 9 - Application non injective

BEATRIX : D'accord, je comprends. Il y a d'ailleurs deux façons équivalentes de dire qu'une application est injective : si $f(x) = f(y)$, alors $x = y$; ou bien, si deux éléments sont différents, alors leurs images sont différentes.

MATHINE : Oui, c'est vrai, Béatrix. Voyons maintenant la surjectivité.

Définition **4.3.4**
Application surjective
On dit qu'une application f d'un ensemble G dans un ensemble H est surjective si pour tout y appartenant à H, il existe un élément x de G tel que $y = f(x)$.

EURISTIDE : Une application surjective, quant à elle, garantit que l'image des éléments de G couvre la totalité de H. Autrement dit, il n'existe pas d'élément de H n'ayant pas d'antécédent par f.

BEATRIX : Ou plus simplement, les éléments de H ont tous un antécédent par f.

EURISTIDE : Alors, qu'en est-il d'une application à la fois injective et surjective ?

MATHINE : C'est l'objet de la définition suivante.

Définition **4.3.5**
Application bijective
On dit qu'une application f est bijective si elle est à la fois injective (cf. 4.3.3) et surjective (cf. 4.3.4).

EURISTIDE : Donc, une application bijective garantit l'association de tout élément de H à un élément et un seul de G par l'application f.

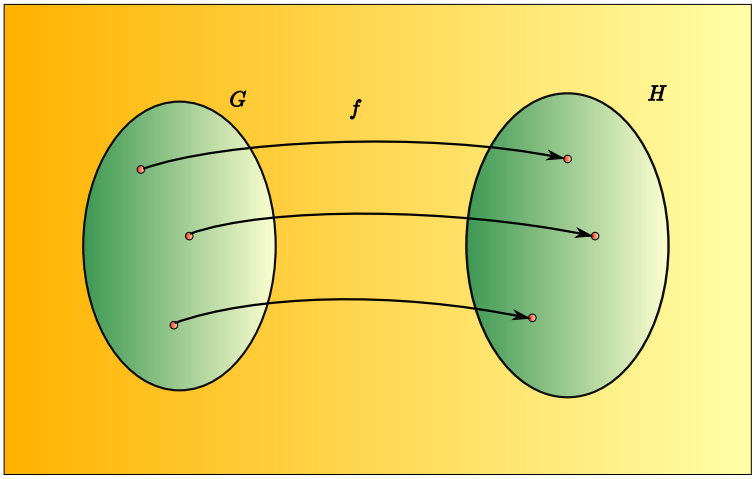

Fig. 10 - Application bijective

BEATRIX : On peut dire en quelque sorte que f transporte point à point l'ensemble G sur l'ensemble H.

EURISTIDE : Oui. Et nous verrons que cela permettra souvent d'identifier l'ensemble G à l'ensemble H.

BEATRIX : Je vois où vous voulez en venir. Je pense que les homomorphismes bijectifs constituent quelque chose de tout à fait intéressant, puisqu'ils vont permettre d'identifier les ensembles, mais aussi les structures, n'est-ce pas ?

MATHINE : Bien vu ! Ce sera l'objectif des isomorphismes de groupes.

Définition **4.3.6**
Isomorphisme de groupe
Soit $(G, \perp)$ et $(H, \top)$ des groupes (cf. 4.1.5). On dit qu'une application $f : G \longrightarrow H$ est un isomorphisme de groupe si f est un homomorphisme (cf. 4.3.1) bijectif (cf. 4.3.5) de G dans H.

EURISTIDE : Nous arrivons donc naturellement à la notion d'isomorphisme. Nous avons vu que l'homomorphisme permettait le transport d'une structure de groupe vers un autre ensemble. L'isomorphisme est la version aboutie et parfaite de ce transport, puisqu'il permet le transport point à point de la structure du groupe G vers H. Deux groupes reliés par un isomorphisme sont dits isomorphes (on le note $G \simeq H$),

et ils sont tellement étroitement liés par ce transport de structure que nous serons régulièrement conduits à les considérer comme identiques. Pour reprendre l'exemple du groupe des entiers relatifs, nous voyons immédiatement que $x \mapsto 2x$ détermine une application surjective et injective du groupe des entiers relatifs $\mathbb{Z}$ vers le groupe des entiers relatifs pairs. En effet, tout élément pair possède une moitié, donc un antécédent par $x \mapsto 2x$. Et deux éléments pairs ne sont égaux que si leurs moitiés sont égales. C'est donc un isomorphisme de groupes, et ces deux groupes se comportent de façon identique vis à vis de la structure de groupe. Les propriétés de $\mathbb{Z}$ sont transportables dans l'ensemble $2\mathbb{Z}$ des entiers relatifs pairs.

MATHINE : Naturellement, nous allons considérer le cas particulier où les deux groupes sont les mêmes, c'est le cas de l'automorphisme.

Définition **4.3.7**
Automorphisme de groupe
Soit $(G, \perp)$ un groupe (cf. 4.1.5). On dit qu'une application f est un automorphisme du groupe G si f est un isomorphisme (cf. 4.3.6) de G dans G.

BEATRIX : Si je comprends bien, l'automorphisme est à l'isomorphisme ce que l'endomorphisme est à l'homomorphisme.

EURISTIDE : Oui, c'est cela. Un automorphisme est donc une application conservant la structure de groupe tout en assurant la correspondance point à point des éléments du groupe.
Par exemple, $f : x \mapsto 2x$ n'est pas un automorphisme dans l'ensemble des entiers relatifs, car les entiers impairs n'ont pas d'antécédent par cette application. Donc f n'y est pas surjective.
En revanche, la même application dans l'ensemble $\mathbb{Q}$ des entiers rationnels est bien un automorphisme.

MATHINE : Voyons maintenant une proposition illustrant la compatibilité entre homomorphisme et structure.

Proposition **4.3.1**
Image de l'inverse par un homomorphisme
Soit $(G, \perp)$ et $(H, \top)$ des groupes (cf. 4.1.5), f un homomorphisme (cf. 4.3.1) de groupes de G dans H. Alors, pour tout x appartenant à G, $f(x^{-1}) = (f(x))^{-1}$.

EURISTIDE : Comme nous l'avons vu, l'homomorphisme conserve la structure de groupe. Cette proposition est donc l'illustration de cette vue, confirmée par la conservation de l'inverse dans le transport effectué par l'homomorphisme.

MATHINE : La démonstration de cette propriété est simple et s'appuie sur la définition de l'homomorphisme et la définition de l'inverse.

Démonstration :

En effet, la démonstration consiste à démontrer que $f(x^{-1})$ est l'inverse de $f(x)$.

Ecrivons, d'une part :

$$f(x\perp x^{-1}) = f(e_G) \quad (91)$$
$$= e_H. \quad (92)$$

D'autre part :

$$f(x\perp x^{-1}) = f(x)\top(f(x))^{-1} \quad (93)$$

Nous avons écrit de deux façons différentes la même expression, donc nous avons :

$$e_H = f(x)\top(f(x))^{-1}. \quad (94)$$

En écrivant de deux façons différentes l'expression $f(x^{-1}\perp x)$, nous obtiendrions, suivant la même méthode que précédemment, le résultat suivant :

$$e_H = (f(x))^{-1}\top f(x). \quad (95)$$

Donc, $(f(x))^{-1}$ est bien l'inverse de $f(x)$.

C.Q.F.D.

Voyons maintenant les notions de noyau et d'image d'un homomorphisme.

Définition **4.3.8**
Noyau d'un homomorphisme
Soit $(G, \perp)$ et $(H, \top)$ des groupes (cf. 4.1.5). Soit f un homomorphisme (cf. 4.3.1) de G dans H. L'ensemble $\{x \in G; f(x) = e_H\}$ est appelé noyau de l'homomorphisme f et noté $Ker(f)$.

BEATRIX : Autrement dit, le noyau est l'ensemble des éléments de G qui s'annulent par f.

EURISTIDE : Nous verrons que la notion de noyau est très importante en Algèbre. Il s'agit effectivement des éléments transportés vers l'élément neutre par l'homomorphisme f.

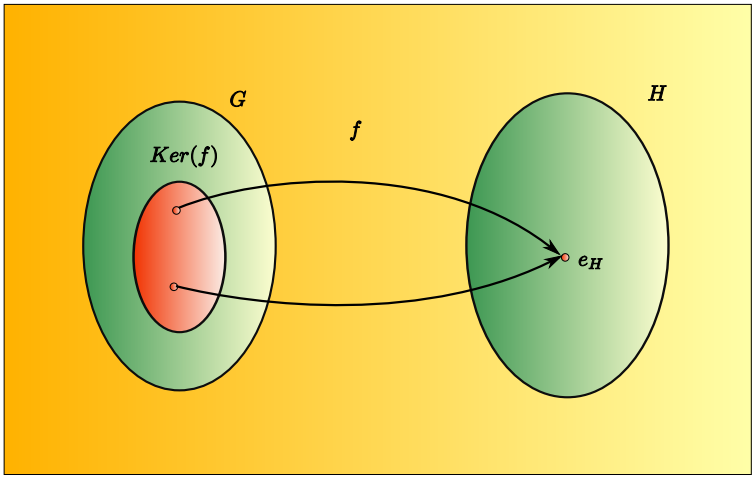

Fig. 11 - Noyau d'un homomorphisme

C'est donc un ensemble d'éléments tout à fait singuliers, qui constituent une classe commune d'éléments ; nous verrons que le terme "classe" que je viens juste d'employer n'est pas anodin, puisque nous pourrons construire une relation d'équivalence en mettant dans une même classe d'équivalence tous les éléments qui sont égaux à un facteur multiplicatif près se trouvant dans le noyau. Autrement dit, ce noyau nous permettra de simplifier la structure d'un groupe G lorsque f n'est pas injective, en considérant uniquement les classes d'éléments regroupant ceux qui ont une image commune.

MATHINE : Nous reviendrons en effet là-dessus tout à l'heure. Dans l'immédiat, poursuivons avec la définition de l'image d'un homomorphisme.

Définition **4.3.9**
Image d'un homomorphisme
Soit $(G, \perp)$ et $(H, \top)$ des groupes (cf. 4.1.5). Soit f un homomorphisme (cf. 4.3.1) de G dans H. L'ensemble $\{y \in H; \exists x \in G; y = f(x)\}$ est appelé image de l'homomorphisme f et noté $Im(f)$.

BEATRIX : Donc, l'image d'un homomorphisme est l'ensemble des éléments de H ayant un antécédent par f.

EURISTIDE : L'image d'un homomorphisme représente en quelque sorte l'impact par l'homomorphisme f de G sur H.

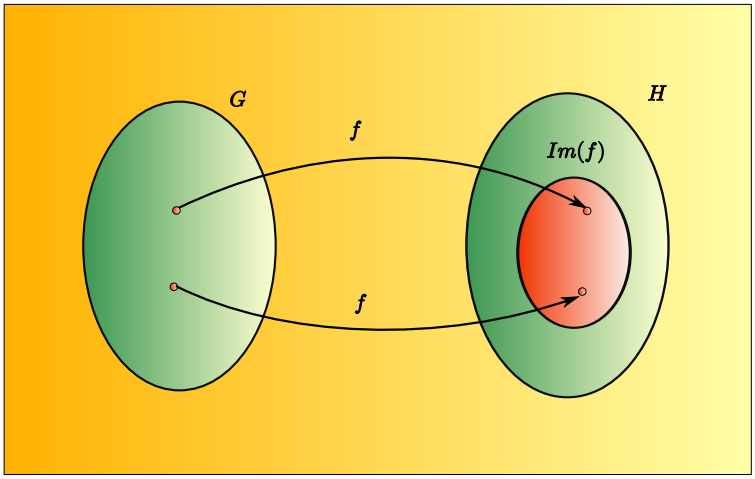

Fig. 12 - Image d'un homomorphisme

En d'autres termes, les éléments de H qui ne se trouvent pas dans $Im(f)$ n'ont pas d'antécédent par f.

MATHINE : Ce que vient de dire Euristide se formalise dans la proposition suivante.

Proposition 4.3.2
Surjectivité et image
Soit f un homomorphisme (cf. 4.3.1) du groupe (cf. 4.1.5) G dans le groupe H. On a équivalence entre :
- *f est surjective (cf. 4.3.4)*
- *$Im(f) = H$.*

Démonstration :

Procédons en deux étapes pour la démonstration de cette équivalence logique.

1) Supposons f surjective.
   Alors, tout élément de H possède un antécédent par f.
   Donc $H \subseteq Im(f)$.
   Or $Im(f) \subseteq H$. Et par conséquent, $H = Im(f)$.
2) Supposons $H = Im(f)$.
   Alors tout élément de H possède un antécédent par f.
   Donc f est surjective.

C.Q.F.D.

BEATRIX : D'accord, c'est clair. Mais, y-a-t-il une proposition similaire pour l'injectivité ?

MATHINE : Oui. Et c'est justement le noyau qui va nous servir de support pour cette proposition.

Proposition 4.3.3
Injectivité et noyau
Soit $(G, \perp)$ et $(H, \top)$ deux groupes. Soit f un homomorphisme (cf. 4.3.1) de G dans H. On a équivalence entre :
- *f est injective (cf. 4.3.3)*
- *$Ker(f)$ est réduit à l'élément neutre (cf. 4.1.3) de G.*

EURISTIDE : Nous avons vu que le noyau représentait les éléments de G qui sont transportés vers l'élément neutre de H par f. On voit effectivement assez bien la relation avec l'injectivité : une application injective ne peut avoir en effet qu'un seul antécédent donné, et par conséquent un homomorphisme injectif aura uniquement l'élément neutre pour antécédent de l'élément neutre de H.

MATHINE : Démontrons cela formellement, en deux étapes puisqu'il s'agit de démontrer une équivalence logique.

Démonstration :

1) Supposons f injective.
Alors, par définition, si x et y sont deux éléments quelconques de G, alors :
$$f(x) = f(y) \Rightarrow x = y. \tag{96}$$
Soit $z \in G$ tel que $f(z) = e_H$, c'est-à-dire $z \in Ker(f)$.
Alors, on peut écrire :
$$f(z - e_G) = f(z) = e_H. \tag{97}$$
D'où, en appliquant la propriété de compatibilité de l'homorphisme :
$$f(z) - f(e_G) = e_H. \tag{98}$$
Ce qui peut s'écrire :
$$f(z) = f(e_G). \tag{99}$$
On en déduit, par l'hypothèse d'injectivité, que :
$$z = e_G. \tag{100}$$
Donc, le noyau $Ker(f)$ est réduit à e_G.
2) Supposons que le noyau $Ker(f)$ est réduit à e_G.
Considérons x et y tels que :
$$f(x) = f(y). \tag{101}$$

Alors :

$$f(x) - f(y) = e_H. \tag{102}$$

D'où :

$$f(x - y) = e_H. \tag{103}$$

Comme $Ker(f) = \{e_G\}$, on en déduit que :

$$x - y = e_G, \tag{104}$$

d'où :

$$x = y. \tag{105}$$

C.Q.F.D.

BEATRIX : Si je fais la synthèse de ces dernières propositions : un homomorphisme injectif a un noyau réduit à l'élément neutre ; un homomorphisme surjectif a une image égale à la totalité du groupe cible.
J'en déduis qu'un isomorphisme a un noyau réduit à l'élément neutre et une image égale à la totalité du groupe cible.

EURISTIDE : Oui, tout à fait, Béatrix. Un isomorphisme va faire correspondre point à point les éléments et la structure des deux groupes, et en particulier les éléments neutres des deux groupes seront mis en relation point à point.

MATHINE : La proposition suivante va nous éclairer sur l'intérêt de la notion de noyau et d'image.

Proposition 4.3.4
Noyau et image sont des sous-groupes
Soit $(G, \perp)$ et $(H, \top)$ deux groupes.
Soit f un homomorphisme (cf. 4.3.1) de G dans H. Alors :
- *$Ker(f)$ est un sous-groupe (cf. 4.2.1) de G.*
- *$Im(f)$ est un sous-groupe de H.*

EURISTIDE : Intuitivement, c'est le fameux transport de structure qui nous permet de comprendre pourquoi $Im(f)$ est un sous-groupe.

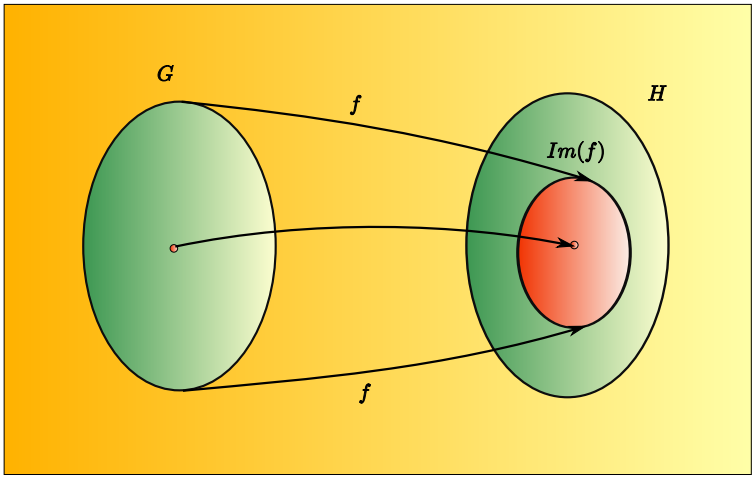

Fig. 13 - Transport du groupe dans l'image

Le fait que le noyau de f soit un sous-groupe découle assez intuitivement lorsqu'on comprend que l'ensemble muni de l'élément neutre dans H est un sous-groupe de H. En remontant le flux de f, on arrive à partir de l'élément neutre de H, à $Ker(f)$, dont la structure de groupe est déduite d'une sorte de contre-transport ou transport retour.

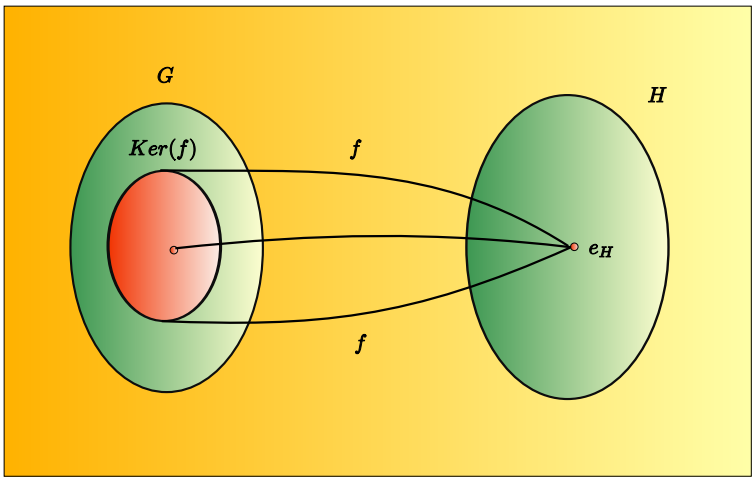

Fig. 14 - Transport retour dans le noyau

BEATRIX : Oui. En raisonnant par l'absurde sur cette même idée, on pourrait dire que si $Ker(f)$ n'était pas un sous-groupe, son image $\{e_H\}$ n'en serait pas un, ce qui serait contradictoire.

MATHINE : Voici la démonstration rigoureuse de cette proposition.

Démonstration :

1) Montrons que $Ker(f)$ est un sous-groupe.
   a) e_G appartient bien à $Ker(f)$, puisque $f(e_G) = e_H$ par définition de l'homomorphisme.
   b) Soit $x, y \in Ker(f)$.
   Considérons l'élément $x \perp y^{-1}$. Alors :

$$\begin{aligned} f(x \perp y^{-1}) &= f(x) \top f(y^{-1}) && (106)\\ &= f(x) \top (f(y))^{-1} && (107)\\ &= e_H \top (e_G)^{-1} && (108)\\ &= e_H \top e_H && (109)\\ &= e_H. && (110) \end{aligned}$$

   Donc $x \perp y^{-1} \in Ker(f)$.
   c) Donc $Ker(f)$ est bien un sous-groupe de G.
2) Montrons que $Im(f)$ est un sous-groupe.
   a) e_F appartient bien à $Im(f)$, puisque $f(e_G) = e_H$.
   b) Soit $x, y \in Im(f)$.
   Considérons l'élément $x \top y^{-1}$.
   Puisque $x \in Im(f)$, il existe $a \in G$ tel que $x = f(a)$.
   Puisque $y \in Im(f)$, il existe $b \in G$ tel que $y = f(b)$.
   Alors :

$$\begin{aligned} x \top y^{-1} &= f(a) \top (f(b))^{-1} && (111)\\ &= f(a) \top f(b^{-1}) && (112)\\ &= f(a \perp b^{-1}). && (113) \end{aligned}$$

   Donc $x \top y^{-1} \in Im(f)$.
   c) Donc $Im(f)$ est bien un sous-groupe de H.

C.Q.F.D.

EURISTIDE : La proposition suivante concerne la composition d'homomorphismes et va nous permettre de transporter les structures de groupe de proche en proche.

MATHINE : Voici comment nous pouvons utiliser la composition d'homomorphismes.

Proposition **4.3.5**
Composition d'homomorphismes
L'application composée de deux homomorphismes (cf. 4.3.1) est un homomorphisme.

Démonstration :

Soit F, G et H trois groupes, dont les lois sont notées $+$ et les éléments neutres e.
Soit $f : F \to G$ et $g : G \to H$ deux homomorphismes.
Soit $x, y \in f$. Alors :

$$g \circ f(x + y) = g(f(x + y)). \tag{114}$$

Puisque f est un homomorphisme, nous en déduisons que :

$$g \circ f(x + y) = g(f(x) + f(y)). \tag{115}$$

Puisque g est un homomorphisme, il s'ensuit que :

$$g \circ f(x + y) = g(f(x)) + g(f(y)). \tag{116}$$

D'où :

$$g \circ f(x + y) = g \circ f(x) + g \circ f(y). \tag{117}$$

Puis :

$$g \circ f(e) = g(f(e)). \tag{118}$$

Puisque f est un homomorphisme :

$$g \circ f(e) = g(e). \tag{119}$$

Et puisque g est un homomorphisme :

$$g \circ f(e) = e. \tag{120}$$

Donc, $g \circ f$ est un homomorphisme.

C.Q.F.D.

4.4 Scène III.4 - Notions supplémentaires sur les groupes

EURISTIDE : Nous allons maintenant regarder comment les groupes peuvent être engendrés à partir d'un nombre réduit d'éléments. C'est un aspect très intéressant car nous allons découvrir des catégories de groupes tels que les groupes monogènes, qui ont des propriétés spécifiques.

BEATRIX : Des groupes monogènes ? Que cela veut-il dire ?

EURISTIDE : Ce sont des groupes qu'on peut générer à partir d'un seul élément.

BEATRIX : Un peu comme une plante que l'on fait germer à partir d'une seule graine.

EURISTIDE : Oui, ici la graine est l'élément générateur, et l'engrais, c'est la loi interne du groupe.

MATHINE : Mais commençons par le début, et définissons ce que signifie engendrer un groupe.

Définition **4.4.1**
Ensemble engendrant un groupe
Soit $(G, \perp)$ un groupe (cf. 4.1.5). Soit I un sous-ensemble de G. On dit que I engendre G si tout élément de G peut s'écrire comme un produit par la loi de groupe d'éléments de I.

EURISTIDE : Par exemple, l'ensemble $\{-1, +1\}$ engendre le groupe des entiers relatifs $(\mathbb{Z}, +)$.

BEATRIX : Oui, parce que tous les éléments de $\mathbb{Z}$ peuvent être déterminés comme une somme d'éléments de $\{-1, +1\}$.
Par exemple :

$$0 = (-1) + 1, \tag{121}$$

et :

$$4 = 1 + 1 + 1 + 1, \tag{122}$$

et enfin :

$$-3 = (-1) + (-1) + (-1). \tag{123}$$

EURISTIDE : Parfois, il peut être nécessaire d'avoir un nombre infini d'éléments pour engendrer un groupe. C'est pourquoi les groupes engendrés par un nombre fini d'éléments, en particulier s'ils sont infinis comme $\mathbb{Z}$ par exemple, ont un caractère remarquable.

MATHINE : C'est l'objet de la définition suivante.

Définition **4.4.2**
Groupe finiment engendré
Soit $(G, \perp)$ un groupe (cf. 4.1.5). On dit que G est finiment engendré s'il existe une partie I de G, de cardinal fini, qui engendre (cf. 4.4.1) G.

EURISTIDE : Pour reprendre l'exemple précédent, nous voyons que l'ensemble fini $\{-1, +1\}$ engendre finiment le groupe infini des entiers relatifs $\mathbb{Z}$.

MATHINE : Introduisons maintenant la notion de cardinal, dont nous allons avoir besoin.

Définition **4.4.3**
Cardinal d'un ensemble
On appelle cardinal d'un ensemble, le nombre d'éléments de cet ensemble. Si un ensemble n'est pas fini, on dit que son cardinal est infini .

EURISTIDE : L'ensemble des entiers relatifs est de cardinal infini. L'ensemble des chiffres, incluant 0, a pour cardinal 10.

MATHINE : Ceci va nous permettre de définir l'ordre d'un groupe.

Définition **4.4.4**
Ordre d'un groupe
On dit qu'un groupe (cf. 4.1.5) est fini si son cardinal est fini. Le cardinal d'un groupe G est noté $|G|$ et est appelé ordre du groupe.

BEATRIX : En bref, l'ordre d'un groupe, c'est son cardinal.

EURISTIDE : En effet. Considérons par exemple l'ensemble $G = \{0, 1, 2, 3\}$. Munissons cet ensemble de la loi $\oplus$ suivante :

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Alors, G est bien un groupe, n'est-ce pas Béatrix ?

BEATRIX : 0 est élément neutre, puisque la première colonne et la première ligne de la table d'addition sont invariantes.
La loi est évidemment associative.
Tout élément x de G a pour inverse $(4 - x)$.

EURISTIDE : C'est donc un groupe fini et son ordre est :

$$|G| = 4. \tag{124}$$

Définissons maintenant le groupe monogène dont nous parlions tout à l'heure.

Définition **4.4.5**
Groupe monogène
On dit qu'un groupe G est monogène s'il est engendre (cf. 4.4.1) par un ensemble constitué d'un unique élément.

EURISTIDE : Le groupe $G = \{0, 1, 2, 3\}$ que nous venons de voir est un exemple de groupe monogène.

BEATRIX : Ah oui, en effet :

$$0 = 1+1+1+1 \quad (125)$$
$$2 = 1+1 \quad (126)$$
$$3 = 1+1+1. \quad (127)$$

Donc, G est engendré par $\{1\}$.

EURISTIDE : Ici, nous avons pris l'exemple d'un groupe monogène fini. Mais un groupe monogène peut être également infini. Par exemple, $\mathbb{Z}$ est un groupe monogène infini. L'élément $\{1\}$ permet de générer $\mathbb{Z}$ entièrement.

MATHINE : Les groupes monogènes qui sont finis portent le nom de groupes cycliques.

Définition **4.4.6**
Groupe cyclique
On dit qu'un groupe G est cyclique s'il est monogène (cf. 4.4.5) et fini (cf. 4.4.4).

BEATRIX : On les appelle cycliques, je suppose, parce qu'en ajoutant indéfiniment l'élément générateur, on obtient un cycle. En reprenant l'exemple du groupe $G = \{0, 1, 2, 3\}$, j'ai :

$$2 = 1+1 \quad (128)$$
$$3 = 1+1+1 \quad (129)$$
$$0 = 1+1+1+1 \quad (130)$$
$$1 = 1+1+1+1+1 \quad (131)$$
$$2 = 1+1+1+1+1+1 \quad (132)$$
$$3 = 1+1+1+1+1+1+1 \quad (133)$$
$$0 = 1+1+1+1+1+1+1+1 \quad (134)$$
$$1 = 1+1+1+1+1+1+1+1+1 \quad (135)$$
$$\ldots = \ldots\ldots\ldots \quad (136)$$

EURISTIDE : Dans ce que tu viens d'illustrer, on voit en particulier dans la suite d'égalités ci-dessus que l'élément neutre 0 revient à intervalle de 4 sommes. C'est le cycle dont tu viens de parler. Dans certains groupes, des éléments peuvent avoir la même propriété de produire l'élément neutre après n opérations. Mathine va nous expliquer cela.

MATHINE : Oui, il s'agit de l'ordre d'un élément.

Définition **4.4.7**
Ordre d'un élément
Soit $(G, \perp)$ un groupe (cf. 4.1.5). Soit g un élément de G. Soit n un élément de $\mathbb{N}^*$.
On note :

$$g^n = \underbrace{g \perp \ldots \perp g}_{n\,fois}. \tag{137}$$

Si $n = 0$, on pose $g^0 = e_G$. Le plus petit élément n de $\mathbb{N}^*$ tel que $g^n = e_G$ est appelé ordre de l'élément g.
Si n est infini, on dira que g est d'ordre infini .

EURISTIDE : Par exemple, dans notre groupe favori $G = \{0, 1, 2, 3\}$, on a :

$$1 + 1 + 1 + 1 = 0, \tag{138}$$

et $1 + 1 \neq 0$, $1 + 1 + 1 \neq 0$, donc l'ordre de 1 est 4.

$$2 + 2 = 0, \tag{139}$$

donc l'ordre de 2 est 2.

$$3 + 3 + 3 + 3 = 0, \tag{140}$$

donc l'ordre de 3 est 4.

BEATRIX : Et dans $(\mathbb{Z}, +)$, l'ordre de 1 est infini.

MATHINE : Voici une proposition appliquant la notion d'ordre d'un élément.

Proposition **4.4.1**
L'ordre d'un élément est inférieur au cardinal du groupe
Si $(G, .)$ est un groupe fini (cf. 4.4.4) alors tout élément de G a un ordre plus petit que le cardinal (cf. 4.4.3) de G.

EURISTIDE : C'est effectivement intuitif. Si on considère chaque produit g^m où m décrit 1 à n (n étant le cardinal de G), au pire chaque g^m est distinct et forcément l'un d'entre eux sera l'élément neutre e de G, puisque G ne comporte au maximum que n éléments distincts.
Si, a contrario, deux éléments g^m et g^l sont égaux, alors si on fait l'hypothèse que $0 \leq l < m \leq n$, on a $g^m = g^l$, soit $g^{m-l} = e$, ce qui nous conduit à la proposition, avec un exposant plus petit que n.

MATHINE : Voyons précisément la démonstration.

Démonstration :

Soit n le cardinal de G.
Procédons par une démonstration par l'absurde.
Supposons que l'élément g ait un ordre m tel que $m > n$.

Alors, nous pourrons construire un ensemble X qui contienne $m-1$ éléments et ne contienne pas l'élément neutre.

$$X = \{g, g^2, \ldots, g^{m-1}\}. \tag{141}$$

Mais comme $X \subset G$, le cardinal de X est nécessairement strictement plus petit que celui de G, puisqu'il ne contient pas e.
Si tous les éléments de X étaient distincts, on aurait $m-1 \leq n-1$, donc $m \leq n$, ce qui contredirait l'hypothèse de départ sur m.
Donc, il existe au moins deux éléments égaux dans X. Notons i et j leurs exposants respectifs :

$$g^i = g^j. \tag{142}$$

Supposons que $i < j$, ce qui ne nuit pas à la généralité. Alors :

$$g^{j-i} = e. \tag{143}$$

Or, $g^{j-i} \in X$ par construction, donc $e \in X$, ce qui contredit l'hypothèse de départ.
Donc $m \leq n$.

C.Q.F.D.

5 Acte IV - Groupes quotients

5.1 Scène IV.1 - Construction d'un groupe quotient

EURISTIDE : Nous avons étudié les ensembles quotients tout à l'heure. Avec le bagage que nous avons acquis, il nous est possible maintenant de regarder l'adaptation de ce concept d'ensemble quotient dans le cadre des groupes.

MATHINE : Nous avons vu qu'il nous fallait une relation d'équivalence. Donc commençons par la définir.

Proposition 5.1.1
Relation d'équivalence du groupe quotient
Soit $(G, .)$ un groupe (cf. 4.1.5), et $(H, .)$ un sous-groupe (cf. 4.2.1) de G. La relation $\mathcal{R}$ définie par $x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$ est une relation d'équivalence (cf. 2.1.4).

BEATRIX : Que signifie cette relation d'équivalence ?

EURISTIDE : Comme toujours, c'est une démarche de simplification, de classification ou d'abstraction. Elle représente une classification des éléments de G par classes réunissant les éléments dont le rapport se trouve dans H. Cela consiste à considérer comme équivalents les éléments qui sont semblables à un facteur multiplicatif près se trouvant dans H.
La relation d'équivalence permet de simplifier la vision que nous avons de G, en regardant les classes d'éléments semblables à un facteur près situé dans H, plutôt que de regarder les individus de G eux-mêmes. C'est ce qui nous permet de définir l'ensemble quotient.

MATHINE : Voici comment nous notons cet ensemble quotient.

Définition **5.1.1**
Notation de l'ensemble quotient
Soit $(G,.)$ un groupe (cf. 4.1.5), et $(H,.)$ un sous-groupe (cf. 4.2.1) de G. Soit $\mathcal{R}$ la relation d'équivalence (cf. 2.1.4) définie par $x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$. On note G/H l'ensemble $G/\mathcal{R}$ des classes d'équivalence (cf. 2.1.5) de la relation $\mathcal{R}$.

EURISTIDE : Cette notation confirme notre discussion. L'ensemble quotient G/H est bien une sorte de simplification modulo H, dont les éléments sont les classes d'éléments semblables entre eux à un facteur multiplicatif près pris dans H.

BEATRIX : Mais à quoi ressemblent ces classes d'éléments ?

MATHINE : C'est la proposition suivante qui va nous le dire.

Proposition **5.1.2**
Expression de la classe d'équivalence
Soit $(G,.)$ un groupe (cf. 4.1.5), et $(H,.)$ un sous-groupe (cf. 4.2.1) de G. Soit $\mathcal{R}$ la relation d'équivalence (cf. 2.1.4) définie par $x\mathcal{R}y \Leftrightarrow x^{-1}y \in H$. La classe d'équivalence (cf. 2.1.5) de x pour la relation $\mathcal{R}$ est l'ensemble $xH = \{x.h; h \in H\}$.

EURISTIDE : Cette proposition exprime bien l'idée que nous nous faisons de la classe d'un élément de x. Comme ce sont les éléments semblables à x à un facteur multiplicatif près pris dans H, il est évident que ce sont les produits de x par un élément h pris dans H, c'est-à-dire les éléments de l'ensemble que nous avons noté xH.

MATHINE : Voici la démonstration de cette proposition. Nous allons procéder en deux étapes pour démontrer l'inclusion dans chacun des deux sens pour déduire l'égalité.

Démonstration :

1) Soit $y \in xH$. Nous allons montrer que y se trouve dans la classe d'équivalence de x.
Puisque $y \in xH$, alors, il existe $h \in H$ tel que :

$$y = xh. \tag{144}$$

Alors, nous pouvons écrire, en multipliant les deux membres de l'égalité par x^{-1} :

$$h = x^{-1}y, \tag{145}$$

par conséquent, $x^{-1}y \in H$.

2) Soit y tel que $x\mathcal{R}y$. Nous allons montrer que y appartient à l'ensemble xH. Puisque $r\mathcal{R}y$, alors $x^{-1}y \in H$. Soit donc $h = x^{-1}y \in H$.
En multipliant les deux membres de l'égalité par x à gauche, on obtient $y = xh$. Donc $y \in xH$.
3) En conclusion, xH est égal à la classe d'équivalence de x pour la relation $\mathcal{R}$.

C.Q.F.D.

BEATRIX : Par exemple, si nous reprenons notre groupe $G = \{0, 1, 2, 3\}$, muni de la loi d'addition $\oplus$. On considère le sous-groupe $\{0, 2\}$, avec la même loi $\oplus$.
La classe de 2 sera l'ensemble des éléments de la forme :

$$2 \oplus 0 = 2 \quad (146)$$
$$2 \oplus 2 = 0. \quad (147)$$

La classe de 3 sera :

$$3 \oplus 0 = 3 \quad (148)$$
$$3 \oplus 2 = 1. \quad (149)$$

La classe de 1 sera :

$$1 \oplus 0 = 1 \quad (150)$$
$$1 \oplus 2 = 3. \quad (151)$$

La classe de 0 :

$$0 \oplus 0 = 0 \quad (152)$$
$$0 \oplus 2 = 2. \quad (153)$$

Nous avons donc simplifié l'ensemble G en considérant deux classes par rapport au sous-groupe $\{0, 2\}$: la classe des éléments pairs $\{0, 2\}$ et la classe des éléments impairs $\{1, 3\}$.

EURISTIDE : Oui, c'est exact.

MATHINE : Nous allons donc maintenant définir cet ensemble xH et son pendant à gauche Hx.

Définition **5.1.2**
Classe à gauche
Soit $(G, .)$ un groupe (cf. 4.1.5). Soit $(H, .)$ un sous-groupe (cf. 4.2.1) de G. Soit x un élément de G. L'ensemble xH (cf. 5.1.2) s'appelle classe à gauche de l'élément x de G.

Définition **5.1.3**
Classe à droite
Soit $(G, .)$ un groupe (cf. 4.1.5). Soit $(H, .)$ un sous-groupe (cf. 4.2.1) de G. Soit x un élément de G. L'ensemble $Hx = \{h.x; h \in H\}$ s'appelle classe à droite de l'élément x de G.

EURISTIDE : Comme la loi de groupe n'est pas toujours commutative, nous sommes en effet amenés à distinguer les classes à droite et les classes à gauche. Evidemment, dans un groupe abélien (dont la loi est donc commutative), cette distinction serait inutile.

BEATRIX : Dans l'exemple que j'ai décrit tout à l'heure, avec $G = \{0, 1, 2, 3\}$, il apparaît que H avait deux éléments, et c'était le cas également des deux classes. Je pense que c'est toujours le cas. Confirmez-vous ?

MATHINE : Nous allons vérifier cela dans la prochaine proposition.

Proposition **5.1.3**
Cardinal des classes à droite et à gauche
Soit $(G, .)$ un groupe (cf. 4.1.5). Soit $(H, .)$ un sous-groupe fini (cf. 4.2.1) de G. Soit x et y deux éléments de G. Alors les ensembles xH, Hx, yH et Hy sont finis et ont même cardinal (cf. 4.4.3) que H.

EURISTIDE : Autrement dit, cette proposition nous confirme qu'il y a autant d'éléments dans H que dans xH et Hx, quel que soit $x \in G$. C'est assez intuitif, dans la mesure où chaque élément de H est remplacé dans xH ou Hx par son produit par x.

MATHINE : Pour démontrer cette proposition, nous allons employer une technique indirecte. Nous allons chercher une bijection entre H et xH. Cela nous permettra de déduire l'égalité des cardinaux.

Démonstration :

Considérons un élément x de G.
Considérons l'application :

$$\begin{array}{rccc} f: & H & \longrightarrow & xH \\ & h & \longmapsto & f(h) = x.h. \end{array} \tag{154}$$

1) Montrons que f est injective.
Soit h et $h' \in H$, tels que :

$$f(h) = f(h'). \tag{155}$$

Alors :

$$x.h = x.h'. \tag{156}$$

Donc, en multipliant cette égalité à gauche par x^{-1}, on obtient :

$$h = h'. \tag{157}$$

Donc :

$$f(h) = f(h') \Rightarrow h = h'. \tag{158}$$

Donc f est injective.

2) Montrons que f est surjective.
Soit $y \in xH$.
Alors, par définition, il existe $h \in H$ tel que :

$$y = x.h, \tag{159}$$

et par conséquent, nous avons trouvé h tel que :

$$y = f(h). \tag{160}$$

Donc, tout élément de xH possède un antécédent par f.
Donc f est surjective.

3) Donc f est injective et surjective.
Donc f est bijective.
Par conséquent, $|H| = |xH|$.

4) Il en serait de même pour Hx, par une démonstration tout à fait similaire à la précédente pour xH.

C.Q.F.D.

BEATRIX : Donc toutes les classes modulo H ont même cardinal, et ont le cardinal de H. Mais ces classes constituent une partition de G, puisqu'elles sont déterminées par une relation d'équivalence. Donc le cardinal de H doit diviser celui de G, n'est-ce pas ?

MATHINE : Excellente déduction, Béatrix. Et ce que tu viens d'expliquer fait l'objet d'un théorème appelé Théorème de Lagrange.

Théorème 5.1.1 (de Lagrange)
Indice d'un sous-groupe
Soit G un groupe fini (cf. 4.4.4). Si H est un sous-groupe (cf. 4.2.1) de G, alors le cardinal (cf. 4.4.3) de H divise celui de G. On notera $|G/H|$ ou $[G : H]$ le nombre $|G|/|H|$. $[G : H]$ s'appelle l'indice de H dans G.

EURISTIDE : Comme tu l'as habilement fait remarquer, on comprend bien cette propriété en considérant par exemple notre groupe $G = \{0, 1, 2, 3\}$. Un sous-groupe de G peut être constitué en considérant les éléments pairs uniquement : $H = \{0, 2\}$. On peut alors constituer, comme tu l'avais illustré, Béatrix, deux classes modulo H seulement : $\{0, 2\}$ et $\{1, 3\}$. L'indice de H dans G est le nombre de classes de la relation d'équivalence modulo H.
Or, ces classes constituent une partition de G. Comme nous avons vu que ces classes ont toutes le même cardinal et que ce cardinal est égal à celui de H, nous en déduisons que le cardinal de H divise le cardinal de G.

MATHINE : Voici la démonstration calquée sur les commentaires de Béatrix et d'Euristide.

Démonstration :

Soit n le nombre de classes modulo H.
Alors, ces classes constituent une partition de G, et ont toutes pour cardinal le cardinal de H. Donc :

$$n|H| = |G|. \tag{161}$$

Par conséquent, $|H|$ divise $|G|$.

C.Q.F.D.

EURISTIDE : On peut en déduire aisément une propriété sur l'ordre d'un élément.

BEATRIX : Oui, je vois. L'ordre d'un élément g, c'est par définition le plus petit $n \in \mathbb{N}^*$ tel que $g^n = e$. Je pense intuitivement que cet ordre doit correspondre à l'ordre du sous-groupe engendré par cet élément. Donc n doit diviser $|G|$ d'après le théorème de Lagrange (cf. 5.1.1).

EURISTIDE : Oui, c'est exact.

MATHINE : Il va nous falloir démontrer un lemme préalablement pour vérifier que l'ordre d'un élément est exactement l'ordre du sous-groupe monogène généré par cet élément.

Lemme **5.1.1**
Ordre d'un sous-groupe monogène
Soit $(G, .)$ un groupe (cf. 4.1.5) fini. Soit $g \in G$ d'ordre (cf. 4.4.4) fini. Alors l'ordre de g est égal à l'ordre du sous-groupe monogène (cf. 4.4.5) engendré par g.

Démonstration :

Les éléments du sous-groupe engendré par g sont de la forme $g^0, g^1, \ldots, g^{m-1}$, où m est l'ordre de ce sous-groupe.
Ce sous-groupe est un groupe cyclique, donc $g^m = g^0 = e$.
Par conséquent, $m - 1$ est le plus grand entier $n \neq 0$ tel que $g^n \neq e$.
Donc m est bien l'ordre de l'élément g.

C.Q.F.D.

EURISTIDE : Ce lemme étant démontré, nous pouvons maintenant énoncer le théorème concernant l'ordre d'un élément.

MATHINE : Le voici.

Théorème **5.1.2**
L'ordre d'un élément divise l'ordre du groupe

Soit G un groupe(cf. 4.1.5). Soit g un élément de G d'ordre fini (cf. 4.4.7). Alors l'ordre de g divise l'ordre (cf. 4.4.4) de G.

EURISTIDE : Cette propriété découle intuitivement du fait que le sous-groupe engendré par chaque élément d'ordre fini du groupe, d'après le Théorème de Lagrange (cf. 5.1.1), est tel que son cardinal divise celui de G. Et il se trouve que l'ordre d'un élément est l'ordre du sous-groupe qu'il engendre d'après le lemme que nous venons de démontrer.

MATHINE : C'est en effet le principe de la démonstration.

Démonstration :

Soit g un élément de G d'ordre m.
Alors, le sous-groupe engendré par g est d'ordre m.
D'après le Théorème de Lagrange (cf. 5.1.1), m divise donc $|G|$.
Par conséquent, l'ordre de l'élément g divise bien l'ordre du groupe.

C.Q.F.D.

EURISTIDE : Avant de parler du plat de résistance que sont les groupes quotients, nous allons avoir besoin d'introduire la notion de sous-groupe distingué.

BEATRIX : A quoi servent les sous-groupes distingués ?

EURISTIDE : C'est une catégorie de sous-groupes pour lesquels nous allons pouvoir confondre les classes à gauche et les classes à droite :

$$\forall x \in G, \quad xH = Hx. \tag{162}$$

C'est donc une forme faible de commutativité au sein d'un sous-groupe. En effet, la véritable commutativité assure l'égalité individuelle de deux éléments $x \in G$ et $h \in H$:

$$xh = hx, \tag{163}$$

alors qu'ici, on garantit seulement collectivement que deux ensembles xH et Hx sont confondus, c'est-à-dire que les ensembles d'éléments sont égaux mais pas forcément les éléments eux-mêmes.

BEATRIX : D'accord, je retiens donc qu'un sous-groupe distingué assure une forme de commutativité faible des éléments de H avec ceux de G, en confondant collectivement les éléments des classes à gauche et à droite.

MATHINE : Voici donc formellement, ce qu'est un sous-groupe distingué.

Définition **5.1.4**
Sous-groupe distingué
Soit G un groupe (cf. 4.1.5). Soit H un sous-groupe de G. On dit que le sous groupe H de G est distingué ou normal dans G si pour tout g dans G et tout h dans H, on a $g.h.g^{-1} \in H$. On note $H \triangleleft G$.

EURISTIDE : Cette définition est différente de la définition reposant sur l'égalité des classes à gauche et à droite. La proposition suivante va donc nous indiquer ce lien.

MATHINE : Oui, cette proposition a pour but de montrer qu'un sous-groupe distingué défini par la définition précédente correspond bien à la forme de commutativité faible expliquée par Euristide.

Proposition **5.1.4**
Classes à gauche/droite confondues pour sous-groupe distingué
Soit G un groupe (cf. 4.1.5). Soit H un sous-groupe (cf. 4.2.1) fini de G. Pour tout x appartenant à G, les classes à gauche xH et à droite Hx sont confondues si et seulement si H est distingué (cf. 5.1.4) dans G.

Démonstration :

Nous démontrerons l'équivalence en démontrant tour à tour les deux implications logiques.

1) Supposons que H est un sous-groupe distingué.
Soit $x \in G$ quelconque.
Montrons que $xH \subseteq Hx$ puis que $Hx \subseteq Hx$.
   a) Montrons que $xH \subseteq Hx$.
   Soit $y \in xH$. Alors il existe $h \in H$ tel que :
   $$y = xh. \tag{164}$$
   Considérons $yx^{-1} = xhx^{-1}$, en multipliant l'égalité précédente à droite par x^{-1}.
   Puisque H est distingué, $xhx^{-1} \in H$.
   Donc $yx^{-1} \in H$.
   Donc, il existe $h' \in H$ tel que :
   $$yx^{-1} = h'. \tag{165}$$
   En multipliant l'égalité à droite par x, on obtient :
   $$yx^{-1}x = y = h'x. \tag{166}$$
   Donc, $y \in Hx$.
   Donc $xH \subseteq Hx$.
   b) Montrons que $Hx \subseteq xH$.
   Soit $y \in Hx$.
   Alors, il existe $h \in H$, tel que :
   $$y = hx. \tag{167}$$
   Considérons :
   $$x^{-1}y = x^{-1}hx, \tag{168}$$

en multipliant l'égalité précédente par x^{-1} à gauche. On peut écrire :

$$x^{-1}y = (x^{-1})h(x^{-1})^{-1}. \tag{169}$$

Puisque H est distingué, $(x^{-1})h(x^{-1})^{-1} \in H$.
Donc :

$$x^{-1}y \in H. \tag{170}$$

Donc, il existe $h' \in H$ tel que :

$$x^{-1}y = h'. \tag{171}$$

D'où, en multipliant l'égalité à gauche par x :

$$y = xh'. \tag{172}$$

Donc $y \in xH$.
Donc $Hx \subseteq xH$.

c) Donc finalement $xH = Hx$.

2) Supposons que pour tout $x \in G$, $xH = Hx$. Montrons que H est distingué dans G.
Soit $h \in H$, soit $g \in G$ quelconque.
Considérons $g.h.g^{-1}$. On peut écrire :

$$ghg^{-1} = (gh)g^{-1}. \tag{173}$$

Or $gh \in gH$, donc $gh \in Hg$, par hypothèse.
Par conséquent, il existe $h' \in H$ tel que :

$$gh = h'g. \tag{174}$$

D'où, en multipliant cette égalité à droite par g^{-1} :

$$\begin{aligned} ghg^{-1} &= h'gg^{-1} && (175)\\ &= h'. && (176)\end{aligned}$$

Donc $ghg^{-1} \in H$.
Donc, H est distingué dans G.

C.Q.F.D.

BEATRIX : C'est effectivement très intéressant, cette notion de sous-groupe distingué et de commutativité au sens faible.

MATHINE : Et cela va être encore plus intéressant quand nous allons découvrir que le noyau d'un homomorphisme est un sous-groupe distingué.

Proposition 5.1.5
Le noyau est un sous-groupe distingué
Soit G, G' deux groupes (cf. 4.1.5). Soit $f : G \longrightarrow G'$ un homomorphisme de groupes. Alors le noyau de f, $Ker(f)$, est un sous-groupe distingué (cf. 5.1.4) de G.

EURISTIDE : Le fait que le noyau d'un homomorphisme de groupes soit un sous-groupe distingué n'est pas étonnant. En effet, par définition de l'élément neutre, le produit d'un élément par l'élément neutre commute. Donc, il est possible de retrouver dans le noyau la forme faible de commutativité où tout élément du noyau multiplié par un élément x du groupe peut être commuté après transport dans G' par f. En effet, ceci est vrai puisque l'on peut faire par l'homomorphisme f un transport aller d'un élément de $xKer(f)$ vers xe'. Ce dernier élément de G' est égal à $e'x$ puisque c'est l'élément neutre de G'. Et le transport retour par la réciproque de f permet de considérer cet élément comme appartenant à la classe à droite du noyau, $Ker(f)x$.
Le schéma ci-dessous illustre ceci : $a \in Ker(f)$ a pour image e', élément neutre de G'. Donc $xa \in xKer(f)$ a pour image xe'. Mais $xe' = e'x$. Donc ax est élément également de la classe à gauche de $Ker(f)$.

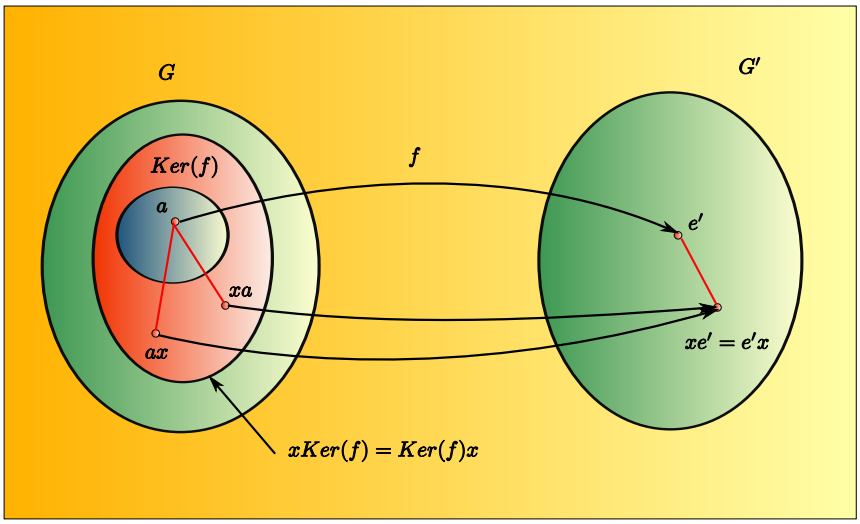

Fig. 15 - Noyau, sous-groupe distingué

MATHINE : Voici donc la démonstration de cette proposition.

Démonstration :

Soit $a \in Ker(f)$.
Considérons $x \in G$ quelconque. Considérons l'élément $x^{-1}ax$.
On a :

$$f(x^{-1}ax) = f(x^{-1}).f(a).f(x) \quad (177)$$
$$= (f(x))^{-1}.f(a).f(x). \quad (178)$$

Or, $f(a) = e'$, puisque $a \in Ker(f)$.
Donc :

$$\begin{aligned} f(x^{-1}ax) &= (f(x))^{-1}.e'.f(x) && (179)\\ &= (f(x))^{-1}.f(x) && (180)\\ &= e'. && (181)\end{aligned}$$

Par conséquent, $x^{-1}ax \in Ker(f)$.
Donc $Ker(f)$ est bien un sous-groupe distingué.

C.Q.F.D.

5.2 Scène IV.2 - Structure de l'ensemble quotient d'un groupe

EURISTIDE : Voilà. Nous avons maintenant le bagage nécessaire pour aborder l'étude du groupe quotient. Parce qu'en effet, nous verrons que l'ensemble quotient est un groupe à condition que le sous-groupe le constituant soit distingué.

BEATRIX : D'accord, je comprends maintenant pourquoi nous avons dû établir ces préliminaires.

MATHINE : Nous allons donc définir la loi induite par le groupe sur l'ensemble quotient.

Définition **5.2.1**
Loi induite sur un quotient
Soit G un groupe (cf. 4.1.5), H un sous-groupe (cf. 4.2.1) de G. Nous considérons l'ensemble quotient (cf. 2.2.1) G/H.
On définit une loi interne (cf. 4.1.1) $\perp$ sur G/H pour tout élément x, y de G par :

$$\overline{x} \perp \overline{y} = \overline{x.y}. \quad (182)$$

Cette loi est appelée loi induite de G sur G/H.

EURISTIDE : Cette démarche est tout à fait significative de ce qu'on a l'habitude de faire en algèbre. Ayant défini un ensemble quotient, donc un ensemble de classes d'équivalence modulo H, c'est-à-dire un regroupement des éléments semblables entre eux à un coefficient multiplicateur près pris dans H, nous pouvons maintenant transporter la loi de G sur cet ensemble quotient en considérant que le produit de deux classes est la classe du produit d'un représentant pris dans chaque classe.
Ainsi, non seulement nous simplifions notre groupe initial en ne regardant que les classes d'individus au lieu des individus eux-mêmes, mais de plus, nous nous intéressons au produit de ses classes, en cohérence avec la structure de groupe initiale, afin de structurer l'ensemble simplifié obtenu.

BEATRIX : Mais, je suppose qu'il va falloir vérifier que la loi définie par Mathine sur l'ensemble quotient a bien un sens. Nous pourrions par exemple craindre que le produit de n'importe quels représentants

x et y de classes $\overline{x}$ et $\overline{y}$ ne soient pas précisément dans la classe du produit xy. Ce n'est pas totalement évident pour moi...

MATHINE : Et tu as tout à fait raison de te méfier, Béatrix. Parce qu'en général, ce n'est pas le cas. Et il faut appliquer une condition à H pour que cela soit bien le cas.

Proposition **5.2.1**
Loi induite définie si sous-groupe distingué
Soit G un groupe (cf. 4.1.5), H un sous-groupe (cf. 4.2.1) de G. La loi induite (cf. 5.2.1) sur l'ensemble quotient (cf. 2.2.1) G/H est définie si et seulement si H est distingué (cf. 5.1.4) dans G.

EURISTIDE : Cette proposition nous indique que la loi de l'ensemble quotient n'existe pas nécessairement. Il faut pour cela une certaine régularité de la loi par rapport à H, c'est-à-dire précisément ce que nous avons appelé la forme faible de commutativité, et que nous avons vue dans le cadre des sous-groupes distingués.
Nous pouvions nous y attendre, parce que pour pouvoir définir la loi, nous avons besoin d'identifier d'une part les produits du type :

$$xh.yh' \tag{183}$$

qui sont les produits d'éléments de deux classes xH, et d'autre part des éléments du type :

$$xyh'' \tag{184}$$

qui sont des éléments de la classe xyH.
Pour pouvoir écrire $xh.yh'$ sous la forme :

$$xh.yh' = xyh'', \tag{185}$$

pour tout h, h', il faut pouvoir en quelque sorte "basculer" h à droite de y, pour réunir h et h' et obtenir ainsi un élément de H que l'on pourra noter h''.
Ce basculement est évidemment toujours possible si la loi est commutative, mais nous n'avons pas besoin d'une condition aussi forte. Il suffit que le sous-groupe soit distingué, offrant ainsi une version plus faible de la commutativité, permettant de remplacer $h.y$ par $y.h'''$.

MATHINE : C'est le principe de la démonstration de cette proposition.

Démonstration :

Puisqu'il s'agit de démontrer une équivalence logique, nous allons effectuer la démonstration en deux étapes pour démontrer les implications logiques dans les deux sens.

1) Supposons que H est distingué.
   Ayant défini la loi :

$$\overline{x} \perp \overline{y} = \overline{xy}, \tag{186}$$

   nous devons vérifier que pour tout élément x' et y' de $\overline{x}$ et $\overline{y}$ respectivement, le produit $x'y'$ se trouve bien dans $\overline{xy}$.
   Considérons donc deux tels éléments :

$$x' \in xH \tag{187}$$
$$y' \in yH. \tag{188}$$

Alors :

$$\exists h \in H, \quad x' = xh, \tag{189}$$

et :

$$\exists h' \in H, \quad y' = yh'. \tag{190}$$

En effectuant leur produit, on a :

$$x'y' = xhyh'. \tag{191}$$

Or :

$$y^{-1}hy \in H, \tag{192}$$

puisque H est distingué dans G.
Donc, on peut écrire :

$$y^{-1}hy = h'', \tag{193}$$

où $h'' \in H$.
Donc $hy = yh''$.
Par conséquent :

$$x'y' = x(hy)h' = xyh''h' = (xy)(h''h'). \tag{194}$$

Donc $x'y' \in (xy)H$.

2) Supposons que la loi :

$$\overline{x} \perp \overline{y} = \overline{xy} \tag{195}$$

soit bien définie, c'est-à-dire que pour tout élément x' et y' de $\overline{x}$ et $\overline{y}$ respectivement, le produit $x'y'$ se trouve bien dans $\overline{xy}$.
Soit $h \in H$. Soit x quelconque élément de G.
Nous devons montrer $x^{-1}hx \in H$.
Pour cela, nous allons montrer que $hx \in xH$.
Or xH est la classe d'équivalence $\overline{x}$ de x.
Nous pouvons écrire :

$$\overline{x} \perp \overline{h} = \overline{xh}. \tag{196}$$

Or :

$$\overline{h} = \overline{e} \tag{197}$$

puisque $h \in H$.
Donc :

$$\overline{xh} = \overline{x} \perp \overline{h} = \overline{x} \perp \overline{e} = \overline{xe} = \overline{x}, \tag{198}$$

et :

$$\overline{hx} = \overline{h} \perp \overline{x} = \overline{e} \perp \overline{x} = \overline{ex} = \overline{x}. \tag{199}$$

Donc :

$$\overline{hx} = \overline{x} = \overline{xh}. \tag{200}$$

Ce qui signifie en particulier que :

$$hx \in \overline{xh}, \tag{201}$$

donc :

$$hx \in xH. \tag{202}$$

C.Q.F.D.

EURISTIDE : Nous avons donc maintenant la possibilité de construire une loi interne. Il ne reste plus qu'un tout petit pas pour définir le groupe quotient.

MATHINE : Et ce pas, nous allons le faire tout de suite.

Théorème 5.2.1
Groupe quotient
Soit G un groupe (cf. 4.1.5). Soit H un sous groupe (cf. 4.2.1) distingué (cf. 5.1.4) de G. Alors l'ensemble quotient (cf. 2.2.1) G/H muni de la loi interne induite (cf. 5.2.1) de celle de G a une structure de groupe. On appelle ce groupe le groupe quotient de G par H. Si G est abélien (cf. 4.1.7), il en est de même de G/H équipé de la loi induite.

Démonstration :

Pour démontrer que G/H est un groupe, nous devons démontrer successivement : que la loi interne induite sur G/H est associative, qu'il existe un élément neutre pour cette loi dans G/H, et que tout élément de G/H possède un inverse pour cette loi induite.

1) Montrons que la loi induite $\perp$ est associative.
Nous avons :
$$(\overline{x}\perp\overline{y})\perp\overline{z} = (\overline{xy})\perp\overline{z} = \overline{(xy)z}. \tag{203}$$
Par associativité de la loi de G, nous avons :
$$(xy)z = x(yz). \tag{204}$$
Donc :
$$\begin{aligned}(\overline{x}\perp\overline{y})\perp\overline{z} &= \overline{x(yz)} &(205)\\ &= \overline{x}\perp(\overline{yz}) &(206)\\ &= \overline{x}\perp(\overline{y}\perp\overline{z}) &(207)\end{aligned}$$
Donc la loi $\perp$ est associative.

2) Montrons que G/H possède un élément neutre pour $\perp$. Nous allons montrer que $\overline{e}$ est l'élément neutre de $\perp$ sur G/H ; soit $\overline{x} \in G/H$ quelconque :
$$\begin{aligned}\overline{x}\perp\overline{e} &= \overline{(xe)} &(208)\\ &= \overline{x}, &(209)\end{aligned}$$
et :
$$\begin{aligned}\overline{e}\perp\overline{x} &= \overline{(ex)} &(210)\\ &= \overline{x}. &(211)\end{aligned}$$
Donc, $\overline{e}$ est bien élément neutre de $\perp$ sur G/H.

3) Montrons que tout élément de G/H possède un inverse. Nous allons montrer que l'inverse de $\overline{x}$ est la classe de l'inverse x^{-1} de x. En effet :

$$\overline{(x^{-1})} \perp \overline{x} = \overline{x^{-1}x} \quad (212)$$
$$= \overline{e}. \quad (213)$$

$$\overline{x} \perp \overline{(x^{-1})} = \overline{xx^{-1}} \quad (214)$$
$$= \overline{e}. \quad (215)$$

Donc $\overline{(x^{-1})}$ est bien l'inverse de $\overline{x}$ et tout élément de G/H possède bien un inverse pour $\perp$.

4) Par conséquent G/H possède bien une structure de groupe pour la loi induite.

C.Q.F.D.

EURISTIDE : Nous arrivons ainsi à définir une structure fondamentale : le groupe quotient attaché à un sous-groupe distingué. Cette structure est très utile, encore une fois, parce qu'elle permet de structurer un groupe simplifié constitué des classes d'éléments modulo H, au lieu de regarder les individus de G eux-mêmes. C'est une démarche de structuration et de simplification qui nous permettra d'effectuer de larges développements à partir des structures de groupes. Il nous faudra donc bien retenir cette notion et sa signification tout au long de nos discussions.

BEATRIX : En résumé, à partir d'un groupe G, on peut considérer les classes d'éléments semblables à un facteur multiplicatif près, pris dans un sous-groupe distingué. Ces classes considérées comme des éléments construisent un groupe, appelé groupe quotient, qui structure cette vue synthétisée par classes du groupe d'origine G.

5.3 Scène IV.3 - Théorèmes d'isomorphisme

EURISTIDE : Oui, c'est bien résumé. Nous allons maintenant aborder quelques théorèmes, appelés théorèmes d'isomorphisme, parce qu'ils établissent des isomorphismes entre groupes et groupes quotients. Bien évidemment, l'intérêt de cette démarche basée sur des isomorphismes, sera la capacité d'identifier deux structures isomorphes entre elles.

BEATRIX : Et je sais maintenant que les mathématiciens aiment faire cela pour enrichir des structures ou en créer de nouvelles.

MATHINE : Commençons donc par définir l'homomorphisme noté Π, qui passe de l'élément à la classe dans une telle structure.

Proposition **5.3.1**
Homomorphisme associant à un élément sa classe

Soit G un groupe (cf. 4.1.5). Soit H un sous-groupe (cf. 4.2.1) de G tel que $H \lhd G$ (cf. 5.1.4). Notons $\Pi : G \longrightarrow G/H$ l'application qui à $x \in G$ associe sa classe d'équivalence (cf. 2.1.5) $\overline{x}$ dans G/H. Alors Π est un homomorphisme de groupe (cf. 4.3.1). De plus $H = Ker(\Pi)$ (cf. 4.3.8) et Π est surjectif (cf. 4.3.4).

`EURISTIDE` : Cette proposition nous permet d'établir une correspondance entre homomorphisme et groupe quotient. Le fait que Π soit surjective est assez prévisible, puisque G/H est un ensemble de classes qui sont non vides, et donc tout élément possède par Π un antécédent qui est un représentant de la classe. Ce qui est intéressant ici, c'est que H soit précisément le noyau de Π.

`BEATRIX` : C'est lié au fait que la classe "neutre" est celle de e, donc H lui-même, n'est-ce pas ?

`EURISTIDE` : Ceci reflète effectivement le fait que H est l'ensemble des représentants de la classe de e, donc la classe neutre du groupe quotient G/H. C'est tout à fait intuitif, puisque la multiplication d'un représentant d'une classe par H ne produit pas de changement de classe par définition des classes qui sont en fait des xH.

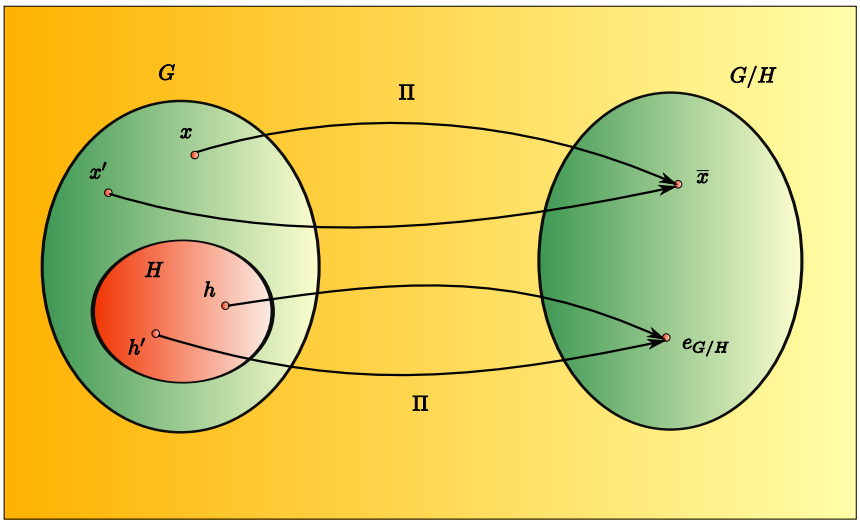

Fig. 16 - Classe neutre du groupe quotient

Dans ce schéma, x et x' sont des représentants de la même classe $\overline{x}$. De même h et h' sont des représentants de la même classe $e_{G/H}$. A noter que $e_G \in H$, donc e_G est un représentant de la classe $e_{G/H}$.

`MATHINE` : Voici la démonstration de cette proposition.

Démonstration :

La démonstration comportera trois étapes : nous commencerons par démontrer que Π est bien un homomorphisme. Puis nous déterminerons son noyau et enfin vérifierons que c'est une surjection.

1) Démontrons que Π est un homomorphisme.
   a) Montrons la compatibilité de l'homomorphisme avec les lois de groupes.
   Comme nous l'avons vu, dans la mesure où H est un sous-groupe distingué, la loi dans G/H :
   $$\overline{x} \perp \overline{y} = \overline{xy} \tag{216}$$
   est bien définie. Donc, en réécrivant l'égalité ci-dessous en utilisant l'expression de Π, nous avons :
   $$\Pi(x) \perp \Pi(y) = \Pi(xy). \tag{217}$$
   ce qui exprime la compatibilité de l'homomorphisme avec les lois de groupes.
   b) Montrons que l'image par Π de l'élément neutre est l'élément neutre de G/H.
   Nous avons vu, par ailleurs, que $e_G \in H$, donc :
   $$\Pi(e_G) = e_{G/H}. \tag{218}$$
   Donc Π est bien un homomorphisme de groupes de G dans G/H.
2) Montrons que H est le noyau de Π.
   $Ker(\Pi)$ est l'ensemble des éléments x de G tels que $\Pi(x) = e_{G/H}$.
   Or, $\Pi(e_G) = e_{G/H}$. Donc $Ker(\Pi) = \overline{e_G}$.
   Par conséquent, par définition de $\overline{e_G}$, $Ker(\Pi)$ est l'ensemble des multiples à gauche d'éléments de H par e_G.
   $$Ker(\Pi) = e_G H. \tag{219}$$
   Donc :
   $$Ker(\Pi) = H. \tag{220}$$
3) Montrons que Π est surjective.
   La surjectivité de Π découle du fait que les classes modulo H constituent une partition de G, et par conséquent, toute classe contient au moins un élément de G.

C.Q.F.D.

EURISTIDE : Nous pouvons maintenant passer au premier théorème d'isomorphisme.

MATHINE : Le voici.

Théorème **5.3.1 (Premier théorème d'isomorphisme)** *Soit G et G' des groupes (cf. 4.1.5). Soit $f : G \longrightarrow G'$ un homomorphisme de groupes (cf. 4.3.1). Rappelons que $Ker(f)$ (cf. 4.3.8) est un sous-groupe (cf. 4.2.1) distingué (cf. 5.1.4) de G, donc $G/Ker(f)$ a une structure de groupe pour la loi induite (cf. 5.2.1) de G. Nous avons également un morphisme surjectif (cf. 4.3.4) $\Pi : G \longrightarrow G/Ker(f)$ qui à tout élément de G associe sa classe d'équivalence (cf. 2.1.5) dans $G/Ker(f)$. De plus, l'image d'un groupe par un morphisme est un sous-groupe du groupe image, donc $Im(f)$ est un sous-groupe de G'. Alors, on peut affirmer qu'il existe un isomorphisme (cf. 4.3.6) $\overline{f} : G/Ker(f) \longrightarrow Im(f)$ tel que $\overline{f} \circ \Pi = \Pi \circ f$.*

EURISTIDE : Voici une illustration de ce théorème.

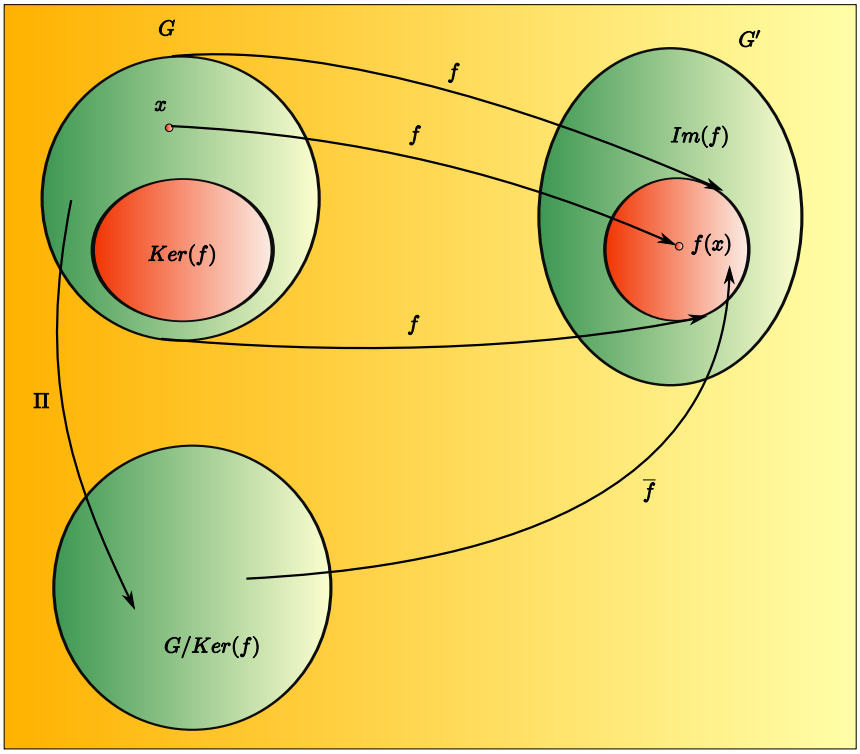

Fig. 17 - Premier théorème d'isomorphisme

Nous avons ainsi construit un isomorphisme entre les classes d'équivalence modulo $Ker(f)$ et l'image de f. C'est tout à fait remarquable, parce que cela nous permet d'identifier les éléments de $G/Ker(f)$ avec ceux de $Im(f)$ à travers cet isomorphisme.
La simplification opérée par ce passage au quotient nous a permis de nous débarrasser des éléments gênants dans G pour f, c'est-à-dire ceux du noyau de l'homomorphisme f, qui révèlent une sorte d'imperfection de l'homomorphisme. Ces éléments possèdent au moins un alter ego dans ce même noyau $Ker(f)$ qui ont une image commune par f.

BEATRIX : Je comprends. Ce sont des empêcheurs de tourner en rond, parce qu'ils interdisent à f d'être injective, et par conséquent interdisent à f d'être bijective sur $Im(f)$.

EURISTIDE : C'est la raison pour laquelle nous faisons ce passage au quotient pour résoudre le problème !

BEATRIX : D'accord. Donc, le réflexe à avoir en algèbre avec un homomorphisme de groupes. Si je veux obtenir un isomorphisme, je passe au quotient modulo $Ker(f)$, et je considère l'homomorphisme induit entre $G/Ker(f)$ et $Im(f)$. Excellente ruse, en effet !

MATHINE : Voici la démonstration de ce premier théorème d'isomomorphisme.

Démonstration :

Nous procéderons en trois étapes. D'abord, nous montrons que si $\overline{f}$ existe, alors il est unique. Puis nous montrons que $\overline{f}$ existe. Puis nous montrons que $\overline{f}$ établit un isomorphisme de $G/Ker(f)$ sur $Im(f)$, en montrant successivement la surjectivité et l'injectivité.

1) Montrons que si $\overline{f}$ existe, alors il est unique.
La condition $\overline{f} \circ \Pi = f$ impose la valeur de $\overline{f}(\overline{x})$ pour tout $\overline{x} \in G/Ker(f)$; cette valeur est $\overline{f}(\overline{x}) = f(x)$.
Donc, si $\overline{f}$ existe, il est déterminé de façon unique, et donc il est unique.
2) Montrons que $\overline{f}$ existe.
Soit x et y deux éléments d'une même classe $\overline{z}$ choisie arbitrairement.
Alors par définition, $xy^{-1} \in Ker(f)$, donc :
$$f(xy^{-1}) = e_{G'}, \tag{221}$$
c'est-à-dire :
$$f(x)(f(y))^{-1} = e_{G'}. \tag{222}$$
Donc :
$$f(x) = f(y). \tag{223}$$
Par conséquent, f est constante sur toute classe $\overline{z}$, quel que soit le représentant choisi dans $\overline{z}$.
C'est ce qui permet de définir la fonction $\overline{f}$ comme étant l'image par f de l'un de ces représentants. $\overline{f}$ peut être définie, puisque cette image ne dépend pas du représentant choisi.
Donc $\overline{f}$ existe.
3) Montrons que $\overline{f}$ établit un isomorphisme de $G/Ker(f)$ sur $Im(f)$.
   a) Surjectivité :
   Soit y un élément quelconque de $Im(f)$. Alors, par définition de $Im(f)$, il existe $x \in G$ tel que :
   $$y = f(x). \tag{224}$$
   Si l'on considère la classe $\overline{x}$ de x, alors nous avons :
   $$\overline{f}(\overline{x}) = f(x) = y. \tag{225}$$
   Donc y a pour antécédent $\overline{x}$ par $\overline{f}$.
   Donc $\overline{f}$ est surjective.
   b) Injectivité :
   Soit $\overline{x}$ et $\overline{y}$ deux éléments de $G/Ker(f)$ tels que :
   $$\overline{f}(\overline{x}) = \overline{f}(\overline{y}). \tag{226}$$
   Par définition de $\overline{f}$, alors :
   $$f(x) = f(y). \tag{227}$$

Donc :

$$f(x)(f(y))^{-1} = e_{G'}, \tag{228}$$

soit :

$$f(xy^{-1}) = e_{G'}. \tag{229}$$

Donc :

$$xy^{-1} \in Ker(f). \tag{230}$$

Et par conséquent, $x \in \overline{y}$, donc :

$$\overline{x} = \overline{y}. \tag{231}$$

Donc $\overline{f}$ est injective.

C.Q.F.D.

EURISTIDE : Voilà. Cette démonstration était relativement simple, et faisait appel à des techniques assez classiques.

BEATRIX : Oui : démonstration de l'unicité, puis de l'existence de la fonction. Puis démonstration de sa bijectivité en démontrant la surjectivité puis l'injectivité, c'est-à-dire en utilisant sa définition.

MATHINE : Passons maintenant au deuxième théorème d'isomorphisme.

Théorème **5.3.2 (Deuxième théorème d'isomorphisme)** *Soit G un groupe (cf. 4.1.5). Soit H et K des sous-groupes (cf. 4.2.1) de G. On suppose $H \triangleleft G$ (cf. 5.1.4). Alors $H \cap K$ est distingué dans K et $K/(K \cap H) \simeq HK/H$.*

BEATRIX : Cette propriété est assez déconcertante en première lecture.

EURISTIDE : C'est vrai. Commençons par l'illustrer pour mieux la comprendre.

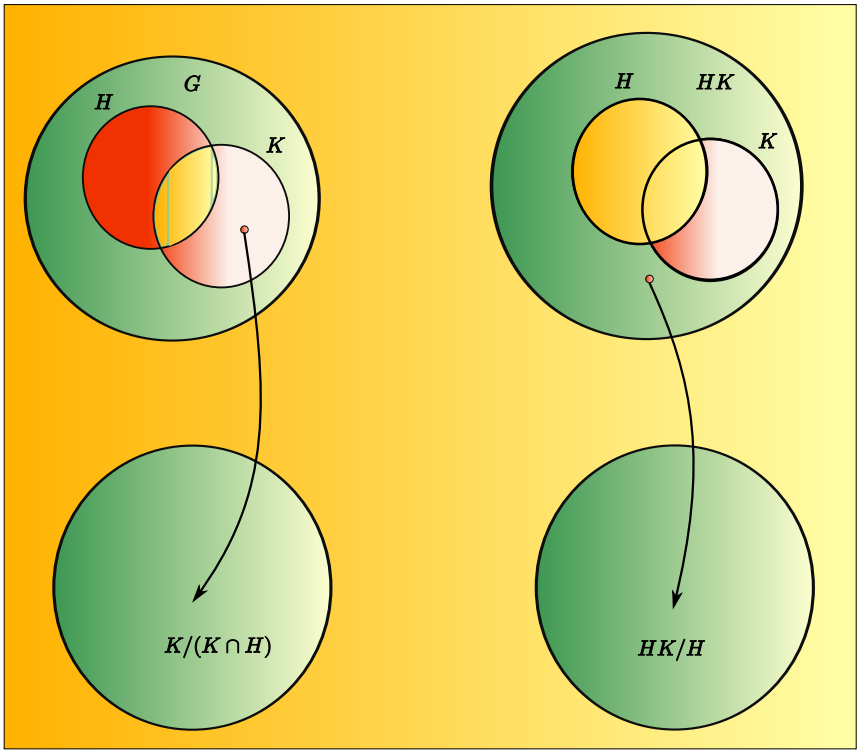

Fig. 18 - Deuxième théorème d'isomorphisme

Analysons maintenant cette construction.
Le passage au quotient $K/(K\cap H)$ permet de regrouper les éléments de K qui sont semblables à un coefficient multiplicateur près, pris dans $K \cap H$. Ces classes sont donc des $k(K \cap H)$, où k est un élément de K.

`BEATRIX` : Ce sont donc des éléments de la forme :

$$kh, \tag{232}$$

où $k \in K$ et $h \in K \cap H$.

`EURISTIDE` : Si nous regardions maintenant le passage au quotient HK/H. Les éléments de HK sont les produits d'éléments de H et de K. Le passage au quotient HK/H permet de regrouper les éléments de HK qui sont semblables à un coefficient multiplicateur près pris dans H. Les classes sont donc des hkH, où h est un élément de H et k un élément de K.

`BEATRIX` : Ce sont donc des éléments :

$$hkh' \tag{233}$$

où $h, h' \in H$ et $k \in K$.
Comment rapprocher ces éléments des classes $k(K \cap H)$?

EURISTIDE : Poursuivons notre analyse. Comme K est stable pour la loi de groupe, les éléments de K peuvent être intuitivement considérés comme des produits d'éléments qui ne se trouvent pas dans $K \cap H$ et d'éléments qui se trouvent dans $K \cap H$, donc des produits d'éléments de $K - (K \cap H)$ et de $K \cap H$. Par conséquent, K est isomorphe au produit $(K \cap H).(K - (K \cap H))$. Le passage au quotient, toujours intuitivement, introduit donc une simplification de même nature que HK/H : en effet, d'une part nous avons :

$$(K \cap H).(K - (K \cap H))/(K \cap H) \simeq K/(K \cap H), \tag{234}$$

et d'autre part, nous avons :

$$HK/H, \tag{235}$$

qui correspondent toutes deux à deux situations semblables où l'on prend le quotient d'un produit AB par son premier terme A, soit AB/A.
L'isomorphisme décrit par le théorème provient de ce parallélisme dans les procédés de simplification entre les deux groupes, donc du parallélisme des passages au quotient.

MATHINE : Bien sûr, l'explication d'Euristide ne constitue pas une démonstration, mais elle éclaire l'équivalence du procédé de simplification entre les deux groupes. Passons maintenant à la démonstration formelle.

EURISTIDE : Pour cela, nous allons utiliser la technique du passage au quotient par le noyau d'un homomorphisme. Il s'agit donc de bien choisir cet homomorphisme. En l'occurrence, nous choisissons l'homomorphisme f défini comme suit :

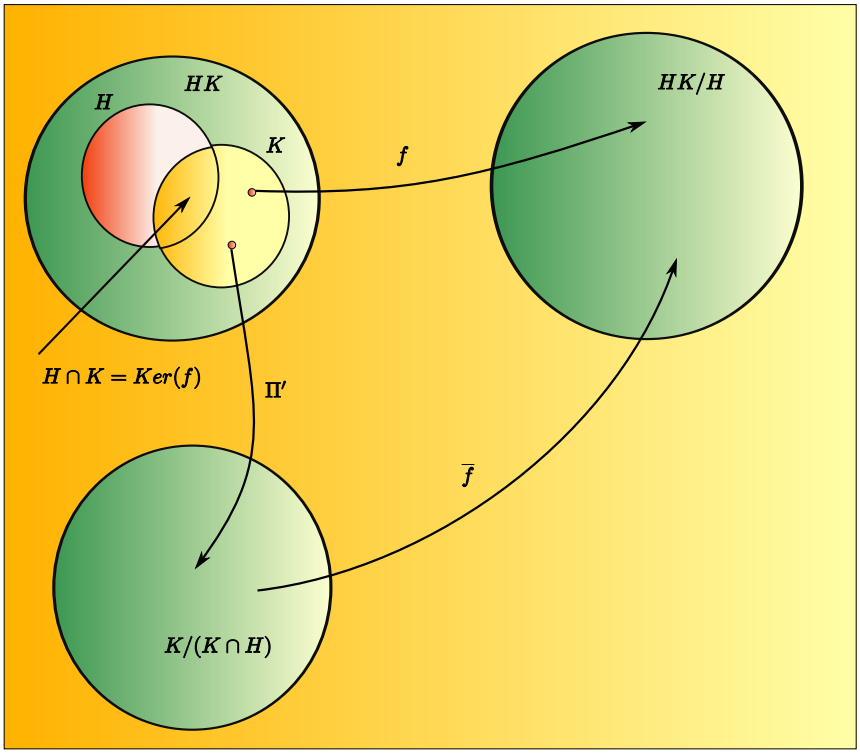

Fig. 19 - Homomorphisme du deuxième théorème d'isomorphisme

MATHINE : Voici donc la démonstration, sur cette base.

Démonstration :

Notons en effet l'homomorphisme f de K dans HK/H qui est la restriction à K de l'homomorphisme :

$$\begin{array}{rccc} \Pi : & HK & \longrightarrow & HK/H \\ & x & \longmapsto & \overline{x}, \end{array} \tag{236}$$

donc :

$$\begin{array}{rccc} f : & K & \longrightarrow & HK/H \\ & x & \longmapsto & \overline{x}. \end{array} \tag{237}$$

1) Surjectivité de f :
Or les éléments de HK/H sont de la forme :

$$\overline{hk}, \tag{238}$$

ou encore :

$$\begin{aligned} \overline{hk} &= \overline{h}.\overline{k} && (239)\\ &= \overline{e}.\overline{k} && (240)\\ &= \overline{k}. && (241) \end{aligned}$$

Donc, nous savons associer à tout élément de HK/H, un élément de K qui en est l'antécédent par f. Donc f est surjective.

2) Sachant cela, étudions maintenant le noyau de f :

$$\begin{aligned} Ker(f) &= \{k \in K, \quad \overline{k} = \overline{e}\} && (242)\\ &= \{k \in K, \quad k \in H\} && (243)\\ &= K \cap H. && (244) \end{aligned}$$

Donc, d'après le premier théorème d'isomorphisme (cf. 5.3.1), le passage au quotient par $K \cap H$ de K nous permet de définir un isomorphisme entre $(K \cap H)/K$ et HK/H.

C.Q.F.D.

BEATRIX : Je comprends mieux, avec l'aide de cette démonstration, la similitude des simplifications entre HK/H et $K/(H \cap K)$. En effet, en simplifiant HK par H, nous pourrions être tentés de croire que le résultat HK/H est équivalent à K. Mais ce n'est pas le cas. Si je considère uniquement les classes d'éléments de K dans HK/H, les éléments de K qui vont se retrouver agglutinés dans une même classe, et par conséquent empêcher la confusion de K et de HK/H, sont ceux qui sont dans H également, et donc dans $H \cap K$. Nous allons donc pouvoir établir un "pont" bijectif entre HK/H et K, à condition de prendre la précaution de simplifier K par les éléments de H qui s'y trouvent.

EURISTIDE : Oui, Béatrix, c'est bien ce qui se passe dans ce deuxième théorème d'isomorphisme.

MATHINE : Voyons maintenant le troisième théorème d'isomorphisme.

Théorème **5.3.3 (Troisième théorème d'isomorphisme)** *Soit G un groupe (cf. 4.1.5). Soit H et K des sous-groupes (cf. 4.2.1)de G. On suppose $H \triangleleft G$ (cf. 5.1.4) et $K \triangleleft G$. On suppose de plus que $H \subset K$. Alors $K/H \triangleleft G/H$ et :*

$$\frac{G/H}{K/H} \simeq G/K. \qquad (245)$$

EURISTIDE : De nouveau, nous allons illustrer cette propriété par un schéma.

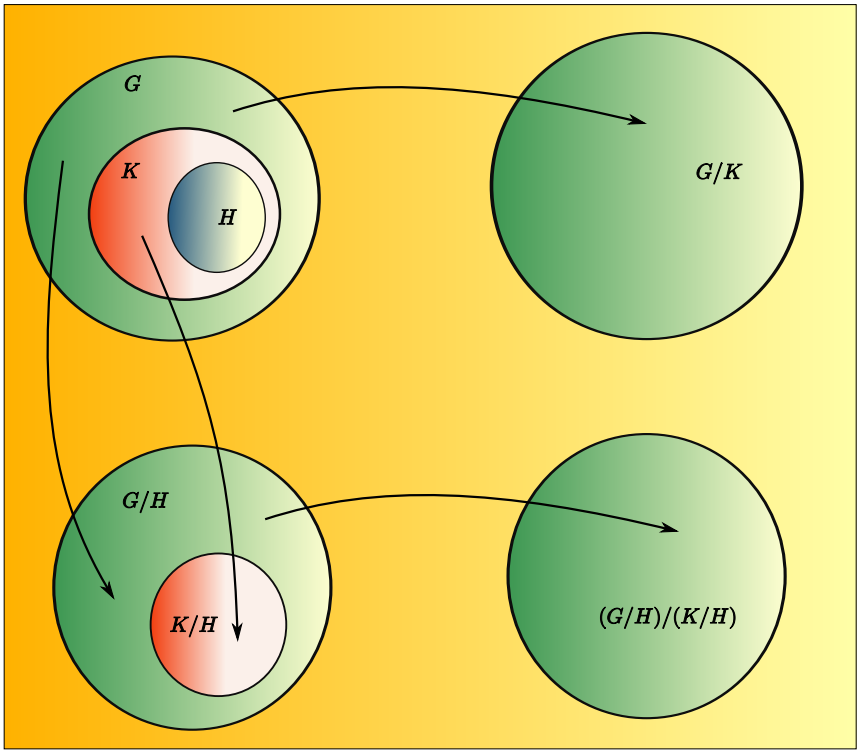

Fig. 20 - Troisième théorème d'isomorphisme

Les éléments de G/H regroupent les éléments de G semblables à un facteur multiplicatif près, pris dans H. Ses classes sont donc les éléments gH où $g \in G$.
Les éléments de K/H regroupent les éléments de K semblables à un facteur multiplicatif près, pris dans H. Ses classes sont les éléments kH où $k \in K$.
Les éléments de $(G/H)/(K/H)$ sont les classes de G/H semblables à un facteur multiplicatif près pris dans K/H. ses classes sont les $x.K/H$, où $x \in G/H$. Donc ses classes sont constituées des éléments $ghkh'$ ou $g \in G$, $k \in K$, et $h, h' \in H$.
Intuitivement, en écrivant ces éléments sous la forme $g.(hkh')$, ceci nous conduit à considérer ces classes comme constituées des éléments de G qui sont semblables à un facteur près se trouvant dans K, puisque hkh' se trouve dans K.
C'est de cette notion intuitive que nous provient l'équivalence entre $(G/H)/(K/H)$ et (G/K).

BEATRIX : On peut facilement se souvenir de cette propriété en imaginant une sorte de loi de simplification des passages au quotient, comme s'il s'agissait de fractions.

EURISTIDE : Oui, mais cette "loi" ne fonctionne qu'à condition que H, K et G soient imbriqués les uns dans les autres dans cet ordre.

MATHINE : Nous allons maintenant démontrer cette propriété.

Démonstration :

Pour réaliser cette démonstration, nous allons de nouveau chercher un homomorphisme dont le noyau nous permettra de construire un espace quotient isomorphe.
Soit f l'homomorphisme de G/H dans G/K défini comme suit :

$$\begin{array}{rccc} f: & G/H & \longrightarrow & G/K \\ & gH & \longmapsto & gK. \end{array} \tag{246}$$

1) Montrons que cet homomorphisme est surjectif.
Soit $\overline{x} \in G/K$. Alors, il existe $g \in G$ tel que :

$$\overline{x} = \{gk; \quad k \in K\}. \tag{247}$$

Alors, si nous considérons l'ensemble :

$$\overline{x_H} = \{gh; \quad h \in H\}, \tag{248}$$

comme $H \subset K$, c'est bien un sous-ensemble de $\overline{x}$ et c'est bien une classe de G/H, donc $\overline{x}$ possède bien un antécédent par f.
Donc f est surjective.

2) Considérons maintenant le noyau de f.

$$Ker(f) = \{\overline{x} \in G/H; \quad f(\overline{x}) = \overline{e}\}. \tag{249}$$

Or, la classe de $\overline{e}$ dans G/K est la classe de K lui-même, donc :

$$\begin{aligned} \overline{x} \in Ker(f) &\Leftrightarrow f(\overline{x}) = \overline{e} && (250)\\ &\Leftrightarrow f(\overline{x}) = K && (251)\\ &\Leftrightarrow \overline{x} = \{gh; \quad g \in K, h \in H\} && (252)\\ &\Leftrightarrow \overline{x} = K/H. && (253) \end{aligned}$$

Donc $Ker(f) = K/H$.

3) Par conséquent, d'après le premier théorème d'isomorphisme, nous pouvons établir un isomorphisme entre G/K et $(G/H)/(K/H)$.

C.Q.F.D.

BEATRIX : De nouveau, tout s'éclaire. Pour établir une bijection entre les classes de G/H et celles de G/K, il y a des classes en trop, qui s'agglutinent dans G/K dans une même classe élément neutre : ce sont les classes de G/H qui ne sont constituées que comme le produit d'un élément de K et tout élément de H. Ces classes correspondent toutes dans G/K à la classe neutre, ce qui est gênant et empêche la correspondance d'être injective et donc d'être bijective. Par conséquent, on se débarrasse de ce problème en passant au quotient.

5.4 Scène IV.4 - Autres définitions

EURISTIDE : Nous allons maintenant passer en revue quelques définitions autour de la commutation des éléments d'un groupe.

MATHINE : Commençons par la définition du centre d'un groupe.

Définition **5.4.1**
Centre d'un groupe
Soit $(G, \perp)$ un groupe(cf. 4.1.5). On appelle centre du groupe G le sous-ensemble de G $\{x \in G; \forall y \in G, \quad x \perp y = y \perp x\}$. On note $Z(G)$ cet ensemble. C'est l'ensemble des éléments de G qui commutent avec tous les autres éléments de G.

EURISTIDE : Dans un groupe non commutatif, il est en effet intéressant de regarder les éléments qui possèdent la propriété de commuter avec tous les éléments du groupe.

BEATRIX : C'est le cas de l'élément neutre, par exemple, n'est-ce pas ?

EURISTIDE : Oui. D'ailleurs, si le groupe est abélien, le centre est le groupe tout entier. Ta remarque va nous permettre d'introduire la proposition suivante.

MATHINE : En effet, le centre d'un groupe s'avère être un sous-groupe. Voici la proposition.

Proposition **5.4.1**
Le centre d'un groupe est distingué
Le centre d'un groupe (cf. 5.4.1) est un sous-groupe (cf. 4.2.1) distingué (cf. 5.1.4) de ce groupe.

EURISTIDE : On pouvait bien entendu s'y attendre, parce que l'élément neutre s'y trouve, et les propriétés de l'inverse d'un élément lui permettent également de commuter.
Le fait que le centre soit distingué se comprend aisément lorsqu'on se souvient qu'un sous-groupe distingué offre une forme faible de commutativité. La présence d'éléments commutant dans un tel sous-groupe assure bien évidemment au moins cette forme faible de commutativité.

MATHINE : Voyons la démonstration qui s'appuie de façon assez élémentaire sur ces remarques, étape par étape.

Démonstration :

1) Montrons que $Z(G)$ est un sous-groupe.

a) Soit $x \in G$ quelconque. On a :

$$ex = xe = x, \tag{254}$$

donc $e \in Z(G)$.

b) Soit $x, y \in Z(G)$.
Alors, soit $z \in G$ quelconque.

$$\begin{aligned}
(xy^{-1})z &= xy^{-1}z && (255)\\
&= x(yz^{-1})^{-1} && (256)\\
&= x(z^{-1}y)^{-1} && (257)\\
&= xzy^{-1} && (258)\\
&= z(xy^{-1}). && (259)
\end{aligned}$$

Donc, $xy^{-1} \in Z(G)$.
Donc, $Z(G)$ est bien un sous-groupe de G.

2) Soit $x \in Z(G)$. Soit y quelconque dans G.

$$\begin{aligned}
y^{-1}xy &= xy^{-1}y && (260)\\
&= xe && (261)\\
&= x. && (262)
\end{aligned}$$

Donc $Z(G)$ est distingué dans G.

C.Q.F.D.

EURISTIDE : Nous avons vu qu'un sous-groupe distingué offre une propriété de commutativité faible, où pour tout $x \in G$:

$$xH = Hx. \tag{263}$$

Il est intéressant de regarder les sous-groupes qui possèdent une telle propriété de commutativité entre eux, c'est-à-dire deux sous-groupes H et K tels qu'il existe un élément $g \in G$, tel que :

$$gH = Kg. \tag{264}$$

MATHINE : Voici la définition des sous-groupes conjugués.

Définition **5.4.2**
Sous-groupes conjugués
Soit G un groupe (cf. 4.1.5). Soit H et K deux sous-groupes (cf. 4.2.1) de G. H et K sont dits conjugués s'il existe un élément g de G tel que $g.H.g^{-1} = K$.

BEATRIX : Cela signifie que deux sous-groupes conjugués sont très proches l'un de l'autre, puisque égaux à un facteur de G près.

EURISTIDE : Oui. Et ta remarque va nous permettre d'énoncer une proposition à leur propos.

MATHINE : Voici la proposition en question.

Proposition **5.4.2**
Bijection entre sous-groupes conjugués
Si deux sous-groupes (cf. 4.2.1) d'un groupe (cf. 4.1.5) G sont conjugués (cf. 5.4.2), alors ils sont en bijection (cf. 4.3.5). Dans le cas où leur cardinal (cf. 4.4.3) est fini, ils ont même cardinal.

Démonstration :

Fixons g tel que $gHg^{-1} = K$.
Considérons la fonction :

$$\begin{array}{rccc} f: & H & \longrightarrow & K \\ & h & \longmapsto & g.h.g^{-1}. \end{array} \tag{265}$$

Alors, démontrons que f est bijective :

1) Surjectivité :
   Soit $k \in K$.
   Comme $K \subset gHg^{-1}$, alors il existe $h \in H$ tel que $k = ghg^{-1}$.
   Donc k possède un antécédent par f.
   Donc f est surjective.
2) Injectivité :
   Soit $h, h' \in H$ tels que $f(h) = f(h')$.
   Alors :

$$ghg^{-1} = gh'g^{-1}. \tag{266}$$

   Multiplions cette égalité à droite par g :

$$ghg^{-1}g = gh'g^{-1}g. \tag{267}$$

   Donc :

$$gh = gh'. \tag{268}$$

   Multiplions à gauche par g^{-1} :

$$g^{-1}gh = g^{-1}gh'. \tag{269}$$

   D'où :

$$h = h'. \tag{270}$$

   Donc f est injective.

C.Q.F.D.

BEATRIX : Oui, c'est assez naturel. H et K se déduisent l'un de l'autre par application d'un facteur unique à gauche et à droite.

MATHINE : Poursuivons par la définition d'un groupe simple.

Définition **5.4.3**
Groupe simple
On dit qu'un groupe (cf. 4.4.3) G est simple si les seuls sous-groupes (cf. 4.2.1) distingués (cf. 5.1.4) de G sont G lui-même et $\{e\}$(cf. 4.1.3).

BEATRIX : Effectivement, de ce point de vue, il n'y a pas plus simple, puisque $\{e\}$ et G sont des sous-groupes distingués inévitables dans tous les groupes.

MATHINE : Voyons maintenant, pour finir dans le domaine des éléments commutants, la notion de commutateur.

Définition **5.4.4**
Commutateur
Soit G un groupe (cf. 4.1.5). Soit g et g' deux éléments de G. On appelle commutateur de g et g' l'élément de G noté $[g, g'] = g.g'.g^{-1}.g'^{-1}$.

BEATRIX : Pourquoi appelle-t-on un tel élément un commutateur ?

EURISTIDE : Nous allons comprendre la raison de ce nom en analysant les propositions ci-après : l'ensemble de ces commutateurs vont permettre de constituer des classes qui appartiennent à un groupe quotient abélien (donc commutatif). Voyons donc les choses dans l'ordre.
La première proposition ci-après nous indique que l'ensemble des commutateurs constitue un sous-groupe distingué, donc permet de construire à partir d'un groupe non abélien, un sous-groupe d'éléments ayant la propriété de commutativité faible des sous-groupes distingués.

MATHINE : Voici la proposition en question, qui permet de définir le sous-groupe dérivé d'un groupe.

Proposition **5.4.3**
Sous-groupe dérivé
Soit G un groupe (cf. 4.1.5). L'ensemble des commutateurs (cf. 5.4.4) des éléments de G engendre un sous groupe (cf. 4.2.1) distingué (cf. 5.1.4) de G appelé sous-groupe dérivé de G et noté $D(G)$.

EURISTIDE : Cette proposition montre ainsi tout l'intérêt et la raison d'être de cette notion de commutateurs. La symétrie engendrée par cette construction permet de constituer un sous-groupe distingué, c'est-à-dire, encore une fois, un sous-groupe dont les éléments possèdent la propriété de commutativité faible, où les classes $xD(G)$ et $D(G)x$ sont confondues.

MATHINE : Mais nous allons pouvoir faire mieux en passant tout à l'heure au quotient. Mais commençons par démontrer cette proposition.

Démonstration :

Soit $x \in D(G)$. Alors x est un produit de commutateurs :

$$x = \prod_{i=1}^{n} [g_i, g_i']. \tag{271}$$

Soit $g \in G$. Alors :

$$\begin{aligned}
gxg^{-1} &= g[g_1, g_1'][g_2, g_2'] \dots [g_n, g_n']g^{-1} && (272)\\
&= gg_1g_1'g_1^{-1}g_1^{'-1}g_2g_2'g_2^{-1}g_2^{'-1} \dots g_ng_n'g_n^{-1}g_n^{'-1}g^{-1} && (273)\\
&= gg_1g_1'(gg^{-1})g_1^{-1}g_1^{'-1}(g^{-1}g)g_2g_2'(gg^{-1})g_2^{-1}g_2^{'-1}(g^{-1}g)\dots && (274)\\
&\quad (g^{-1}g)g_ng_n'(gg^{-1})g_n^{'-1}g^{-1} && (275)\\
&= (gg_1)(g_1'g)(gg_1)^{-1}(g_1'g)^{-1}(gg_2)(g_2'g)(gg_2)^{-1}(g_2'g)^{-1} && (276)\\
&\quad \dots (gg_n)(g_n'g)(gg_n)^{-1}(g_n'g)^{-1} && (277)\\
&= \prod_{i=1}^{n} [gg_i, g_i'g]. && (278)
\end{aligned}$$

Donc, $gxg^{-1} \in D(G)$.
Donc $D(G)$ est distingué.

C.Q.F.D.

BEATRIX : Oui, je comprends. La structure même du commutateur permet de propager la combinaison gg^{-1} sur chaque commutateur constituant un élément de $D(G)$. Ainsi, la structure de produit de commutateur peut être conservée.

EURISTIDE : A noter une propriété intéressante des commutateurs. A ton avis, Béatrix, que représente $[g', g]$ par rapport à $[g, g']$?

BEATRIX : Je ne sais pas.

EURISTIDE : Multiplie-les ensemble...

BEATRIX : Alors, voyons :

$$\begin{aligned}
[g,g'].[g',g] &= gg'g^{-1}g'^{-1}g'gg'^{-1}g^{-1} && (279)\\
&= gg'g^{-1}(g'^{-1}g')gg'^{-1}g^{-1} && (280)\\
&= gg'g^{-1}gg'^{-1}g^{-1} && (281)\\
&= gg'(g^{-1}g)g'^{-1}g^{-1} && (282)\\
&= gg'g'^{-1}g^{-1} && (283)\\
&= g(g'g'^{-1})g^{-1} && (284)\\
&= gg^{-1} && (285)\\
&= e. && (286)
\end{aligned}$$

Donc $[g',g]$ est l'inverse de $[g,g']$.

EURISTIDE : Oui, c'est à retenir :

$$([g,g'])^{-1} = [g',g]. \quad (287)$$

BEATRIX : J'ai compris aussi que si le groupe G est abélien, son sous-groupe des commutateurs est réduit à $\{e\}$, puisque dans ce cas, tout commutateur est réduit à e.

MATHINE : Nous allons maintenant construire un groupe abélien à l'aide de ces commutateurs.

Proposition 5.4.4
Plus grand quotient abélien
Soit G un groupe (cf. 4.1.5). $G/D(G)$ est le plus grand quotient (cf. 5.2.1) abélien (cf. 4.1.7) de G.

EURISTIDE : On voit ici, avec cette proposition, l'intérêt de cette notion de commutateur et de sous-groupe dérivé. En passant au quotient, donc en considérant les classes d'éléments semblables à un coefficient produit de commutateurs près, on obtient un groupe quotient abélien, et de plus, c'est le plus grand que l'on puisse construire.

BEATRIX : Comment cela se fait-il ?

EURISTIDE : Pour comprendre cela, prenons deux éléments $\overline{x}$ et $\overline{y}$ de ce groupe quotient. Ce sont des ensembles du type $xD(G)$ et $yD(G)$.
En développant deux éléments de ces classes, on obtient :

$$\overline{x} = \{z \in G; \quad \exists g_i, g'_i \in G, i \in [1,n], z = x\prod_{i=1}^{n}[g_i,g'_i]\} \quad (288)$$

$$\overline{y} = \{z' \in G; \quad \exists h_i, h'_i \in G, i \in [1,m], z' = y\prod_{i=1}^{m}[h_i,h'_i]\}. \quad (289)$$

Si on regarde un élément zz', on a :

$$\begin{aligned} zz' &= x\prod_{i=1}^{n}[g_i, g_i']y\prod_{i=1}^{n}[h_i, h_i'] && (290)\\ &= xg_1g_1'g_1^{-1}g_1^{'-1}\dots g_ng_n'g_n^{-1}g_n^{'-1}yh_1h_1'h_1^{-1}h_1^{'-1}\dots h_mh_m'h_m^{-1}h_m^{'-1} && (291)\\ &= (xy)(y^{'-1}g_1)(g_1'y^{-1})(y^{-1}g_1)^{-1}(g_1'y^{-1})^{-1}\dots && (292)\\ &\quad (y^{-1}g_n)(g_n'y^{-1})(y^{-1}g_n)^{-1}(g_n'y^{-1})^{-1}(y^{-1}y)h_1h_1'h_1^{-1}g_1^{'-1}\dots && (293)\\ &\quad h_mh_m'h_m^{-1}h_m^{'-1} && (294)\\ &= (xy)\prod_{i=1}^{n}[y^{-1}g_i, g_i'y^{-1}]\prod_{i=1}^{m}[h_i, h_i']. && (295) \end{aligned}$$

On voit donc que la structure des commutateurs permet encore de déplacer le y du milieu de l'expression vers la gauche, ce qui permet à zz' d'être de la forme requise pour appartenir à $D(G)$, et par conséquent aux classes $\overline{xy}$ et $\overline{yx}$ d'être identiques.

`BEATRIX` : C'est ce qui permet au groupe des classes, donc au groupe quotient, d'être abélien. Mais pourquoi est-ce le plus grand ?

`EURISTIDE` : Par nature, les seuls commutateurs non triviaux (c'est-à-dire non égaux à l'élément neutre) sont ceux construits sur des éléments de G qui ne commutent pas entre eux. Donc la simplification opérée par le passage au quotient s'effectue strictement sur les seuls éléments non commutants, et pas plus. C'est en ce sens qu'il faut comprendre qu'on obtient la structure abélienne la plus grande possible.

`BEATRIX` : C'est assez astucieux. Si je résume : les commutateurs non réduits à l'élément neutre sont ceux construits à partir d'éléments non commutants. Le passage au quotient constitue une simplification du groupe G permettant de se débarrasser de ces éléments gênants qui ne commutent pas, et d'obtenir ainsi le plus grand groupe quotient abélien possible. C'est diabolique !

`MATHINE` : Pas tant que cela. La démonstration va nous permettre de vérifier que Lucifer est innocent dans cette affaire.
La démonstration va comporter deux étapes. D'une part vérifier que $G/D(G)$ est abélien, et d'autre part vérifier que si H est distingué dans G et G/H est abélien, alors $D(G) \subset H$, ce qui permettra de déduire qu'un quotient par $D(G)$ est le plus grand qu'on puisse concevoir.

Démonstration :

1) Montrons que $G/D(G)$ est abélien.
Soit $\overline{x}, \overline{y} \in G/D(G)$. Alors, comme $[x, y] \in D(G)$, on a :

$$\begin{aligned} \overline{[x,y]} &= \overline{e} && (296)\\ &= \overline{xyx^{-1}y^{-1}} && (297)\\ &= \overline{xy}\,\overline{x^{-1}y^{-1}}. && (298) \end{aligned}$$

Donc :

$$\overline{e} = \overline{xy}\,\overline{x^{-1}y^{-1}}. \quad (299)$$

D'où, en multipliant par $\overline{yx}$ à droite :

$$\overline{yx} = \overline{xy}\overline{x^{-1}y^{-1}}\overline{yx}, \tag{300}$$

soit :

$$\overline{yx} = \overline{xy}\overline{x^{-1}y^{-1}yx}, \tag{301}$$

soit :

$$\overline{yx} = \overline{xy}. \tag{302}$$

Ou encore :

$$\overline{yx} = \overline{xy}. \tag{303}$$

Donc, $G/D(G)$ est bien abélien.

2) Soit H un sous-groupe distingué de G tel que G/H soit abélien. Rappelons que le fait que H soit distingué dans G est une condition nécessaire pour que l'ensemble quotient par H soit un groupe.
Considérons $x, y \in G$ quelconques.
Soit $\overline{x}, \overline{y}$ les classes de x et y dans G/H.
Alors, puisque G/H est abélien par hypothèse, on a :

$$\overline{xy} = \overline{yx}. \tag{304}$$

Par conséquent :

$$\overline{xy}\overline{x^{-1}y^{-1}} = \overline{e}. \tag{305}$$

Donc :

$$\overline{xyx^{-1}y^{-1}} = \overline{e}. \tag{306}$$

On en déduit que :

$$\overline{[x,y]} = \overline{e}, \tag{307}$$

donc $[x,y] \in H$, puisque la classe neutre est constituée des éléments de H.
Comme x, y sont quelconques, cela signifie que tout commutateur appartient à H.
Par conséquent, tout produit de commutateurs appartient également à H, et donc :

$$D(G) \subseteq H. \tag{308}$$

Donc $D(G)$ est le plus petit sous-groupe distingué de G, permettant de construire un quotient abélien. Par conséquent, son quotient est le plus grand.

C.Q.F.D.

6 Acte V - Action de groupe

6.1 Scène V.1 - Définition

EURISTIDE : Nous allons maintenant passer à l'étude des actions de groupe. L'idée provient de la situation suivante. Supposons que nous ayons un ensemble quelconque, non structuré, que nous appellerons X. A côté de cet ensemble, nous pouvons avoir un groupe, par exemple un groupe additif $\{0,1,2,3,4,5\}$. Il peut être intéressant de regarder ce qui se passe sur l'ensemble X lorsque chaque élément du groupe produit une action sur les éléments de X. Par exemple, si X est un ensemble de lettres $\{A,B,C,D,E,F\}$, on va

décider que l'élément 1 du groupe nous fait passer à la lettre suivante, en considérant que lorsqu'on arrive à F, on passe ensuite à A. L'élément 2 nous fera passer en avant de deux lettres, etc. En s'arrangeant pour que cette action de groupe sur l'ensemble de lettres soit cohérente avec la structure de groupe, c'est-à-dire que si j'applique l'action de l'élément 1 puis de l'élément 2 du groupe sur un élément de l'ensemble X, le résultat sera le même que lorsque j'applique l'action de l'élément du groupe $3 = 1 + 2$. C'est cela que j'appelle la cohérence de la loi de groupe avec l'action.

BEATRIX : Si je comprends bien, la structure de groupe va permettre d'agir sur les éléments de X, et les faire bouger en cohérence avec la loi de groupe.

MATHINE : Voici la définition formelle d'une action de groupe.

Définition **6.1.1**
Action d'un groupe
Soit X un ensemble. Soit G un groupe (cf. 4.1.5). On dit que le groupe G agit ou opère sur l'ensemble X s'il existe une application $\theta : G \times X \longrightarrow X$ telle que :
- *Pour tout x dans X, $\theta(e, x) = x$.*
- *Pour tout $g1, g2 \in G$, $\theta(g1, \theta(g2, x)) = \theta(g1.g2, x)$.*

On dit aussi que θ définit une action de G sur X.
On note $\theta(g, x) = g.x$.

EURISTIDE : L'action d'un groupe sur un ensemble porte donc bien son nom. Les éléments du groupe modifient les éléments de l'ensemble, ou les déplacent, comme s'ils agissaient dessus. Comme je l'ai dit précédemment, comme G est un groupe, il faut que cette action soit cohérente avec la structure de groupe : la première propriété de la définition garantit que l'élément neutre du groupe agit en laissant invariants les éléments de l'ensemble X ; la seconde propriété de la définition nous assure de la compatibilité de cette action avec la loi de groupe : agir successivement avec deux éléments du groupe est la même chose qu'agir avec leur produit.

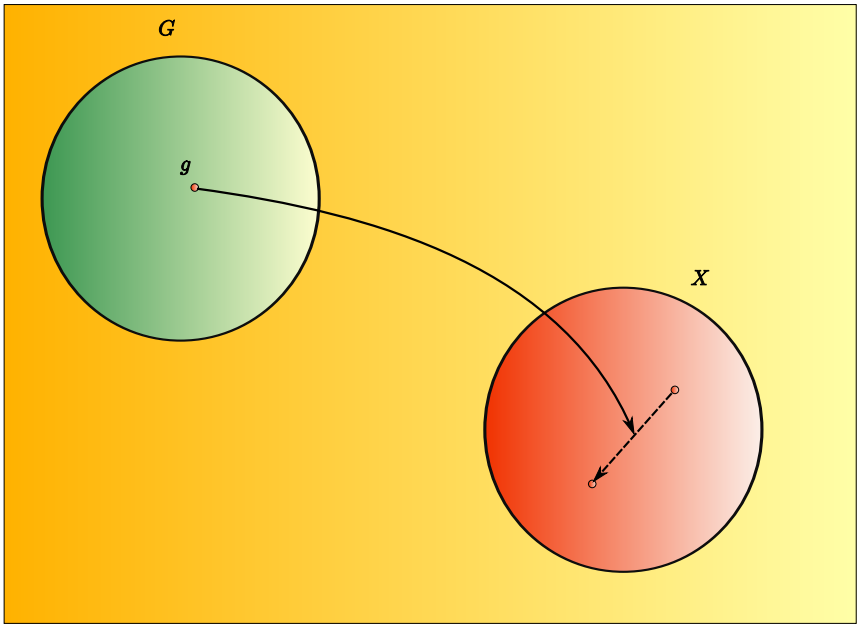

Fig. 21 - Action de groupe

BEATRIX : J'ai un exemple en tête. Si l'ensemble X est l'espace affine euclidien, dans lequel on définit des points et des figures de la géométrie euclidienne, et si le groupe G est le groupe des rotations autour du point 0 de X, alors on peut faire agir G sur X, en faisant une rotation des figures géométriques autour de l'origine 0.

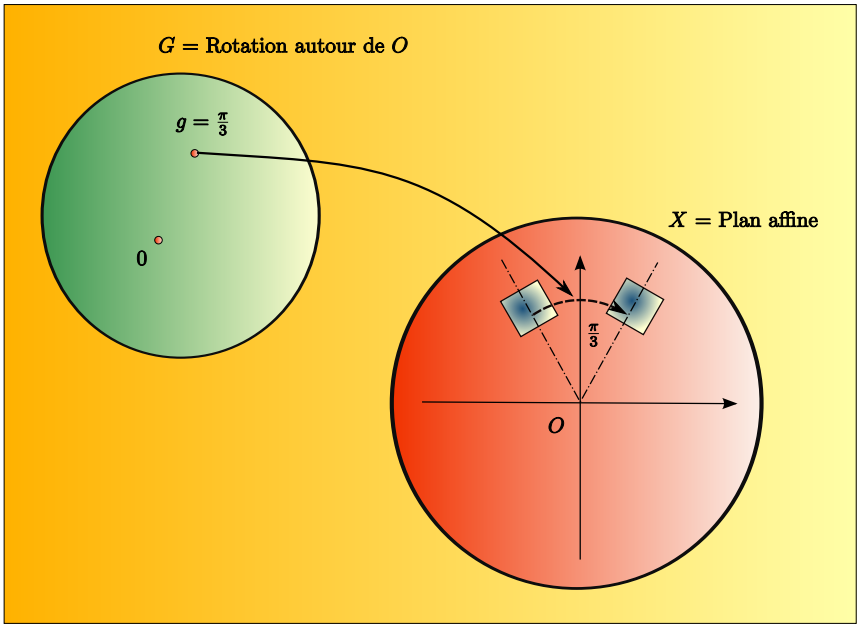

Fig. 22 - Action par rotation

On voit que le groupe des rotations agissant sur le plan affine est bien compatible avec la loi de groupe qui est la loi de composition des rotations.

BEATRIX : Nous avons vu que pour l'action d'un groupe, X devait être invariant par l'action de l'élément neutre du groupe. Inversement, nous pouvons nous demander s'il existe des actions de groupe où seul l'élément neutre est invariant sur X.

MATHINE : C'est l'objet de la définition suivante.

Définition **6.1.2**
Action fidèle
Soit X un ensemble. Soit G un groupe (cf. 4.1.5). Soit θ une action (cf. 6.1.1) de G sur X. On dit que l'action est fidèle si θ vérifie : $\forall x \in X; g.x = x \Rightarrow g = e$.

EURISTIDE : L'action fidèle est donc un niveau de perfectionnement supplémentaire, garantissant que les éléments du groupe ont effectivement toujours une action sur X, à l'exception de l'élément neutre.

BEATRIX : Donc, pour une action fidèle, on peut dire en quelque sorte que l'équation :

$$g.x = x \tag{309}$$

peut se simplifier en :

$$g = e. \tag{310}$$

EURISTIDE : On peut également se poser une question supplémentaire : les éléments de l'ensemble X sont-ils tous atteignables par l'action du groupe. Autrement dit, l'action de groupe garantit-elle qu'elle va atteindre tous les éléments de X ? Ou encore mieux : l'action de groupe garantit-elle qu'elle va permettre de relier deux éléments quelconques de X ?

MATHINE : C'est l'objet de la définition de l'action transitive.

Définition **6.1.3**
Action transitive
Soit X un ensemble. Soit G un groupe. Soit θ une action de G sur X. On dit que l'action est transitive si $\forall x, y \in X; \exists g \in G; g.x = y.$

BEATRIX : Oui, donc en résumé, l'action transitive permet de relier n'importe quel couple d'éléments de X en choisissant le bon élément de G pour l'action.

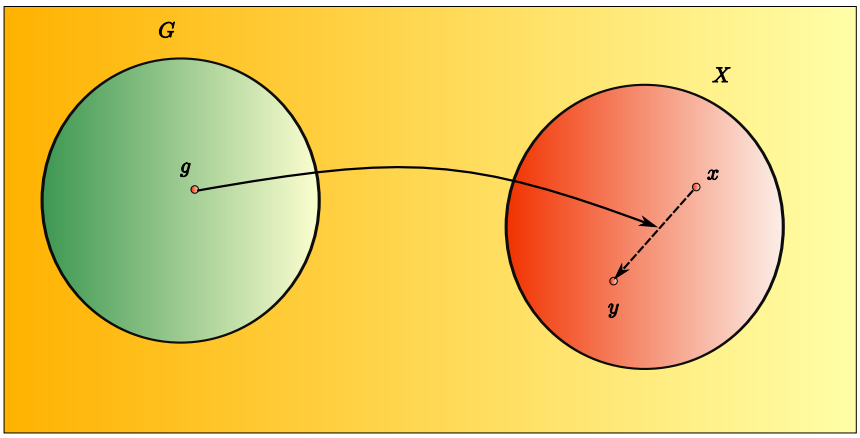

Fig. 23 - Action transitive

EURISTIDE : Nous allons maintenant parcourir un certain nombre d'ensembles particuliers attachés à la notion d'action de groupe, en particulier lorsqu'on fixe l'élément de l'action g de G, ou lorsqu'on fixe l'élément destination de X.

MATHINE : Commençons par fixer un élément de X et regardons quels sont les éléments de G qui maintiennent cet élément.

Définition **6.1.4**
Stabilisateur
Soit X un ensemble. Soit G un groupe (cf. 4.1.5). Soit θ une action (cf. 6.1.1) de G sur X. Soit x un élément de X. On appelle stabilisateur de x le sous-ensemble de G donné par $stab(x) = \{g \in G; g.x = x\}$.

EURISTIDE : Le stabilisateur de x est donc le sous-ensemble de G n'ayant pas d'action sur x.

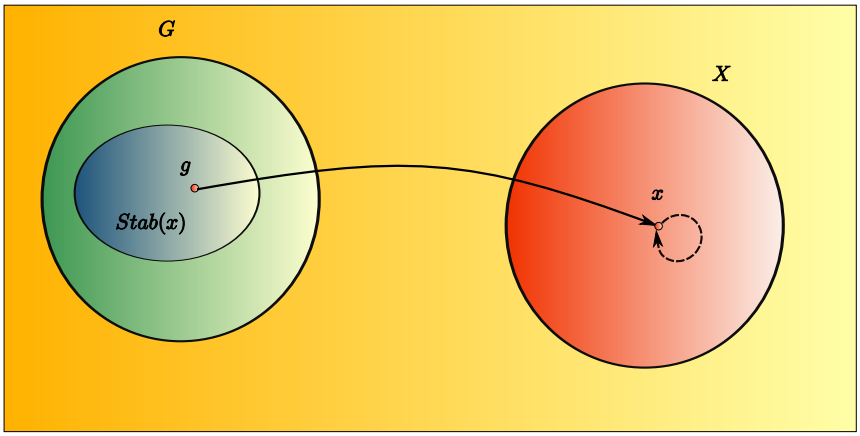

Fig. 24 - Stabilisateur

BEATRIX : Bien entendu, si l'action est fidèle, le stabilisateur de x est réduit à l'élément neutre de G. Par ailleurs, les stabilisateurs contiennent toujours l'élément neutre. Peut-être sont-ce des sous-groupes ?

MATHINE : Nous verrons cela plus tard. Voyons pour l'instant l'ensemble des images d'un point de X par l'action de tous les éléments de G.

Définition **6.1.5**
Orbite

Soit X un ensemble. Soit G un groupe (cf. 4.1.5). Soit θ une action (cf. 6.1.1) de G sur X. Soit x un élément de X. On appelle orbite de x le sous-ensemble de X donné par $w(x) = \{g.x; g \in G\}$.

EURISTIDE : Le nom d'orbite est assez symbolique, car cet ensemble représente tous les transports possibles de x sous l'action de G.

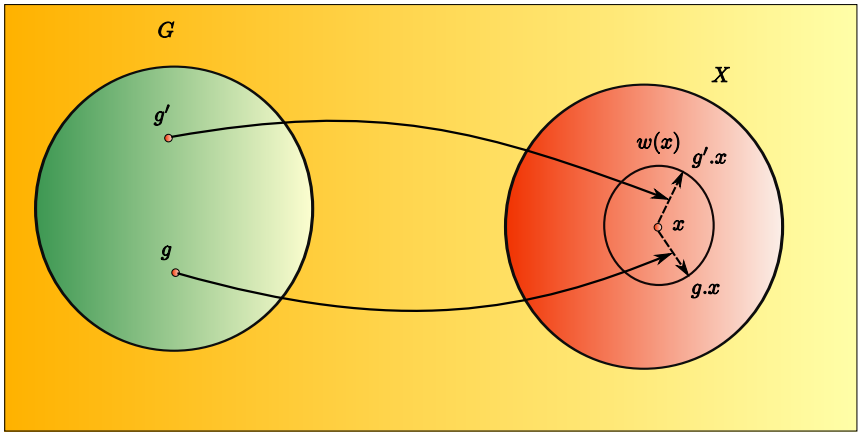

Fig. 25 - Orbite

MATHINE : Voyons maintenant le fixateur d'un élément de g.

Définition **6.1.6**
Fixateur
Soit X un ensemble. Soit G un groupe (cf. 4.1.5). Soit θ une action (cf. 6.1.1) de G sur X. Soit g un élément de G. On appelle fixateur de g, et on note $fix(g)$ ou X^g, le sous-ensemble de X donné par $fix(g) = \{x \in X; g.x = x\}$. De même, si K est une partie de G, on notera X^K l'ensemble des $x \in X$ tels que $\forall g \in K; g.x = x$.

EURISTIDE : Le fixateur d'un élément g de G est l'ensemble des éléments de X invariants sous l'action de g.

BEATRIX : Ce sont, en bref, les éléments de X qui fixent l'action de g.

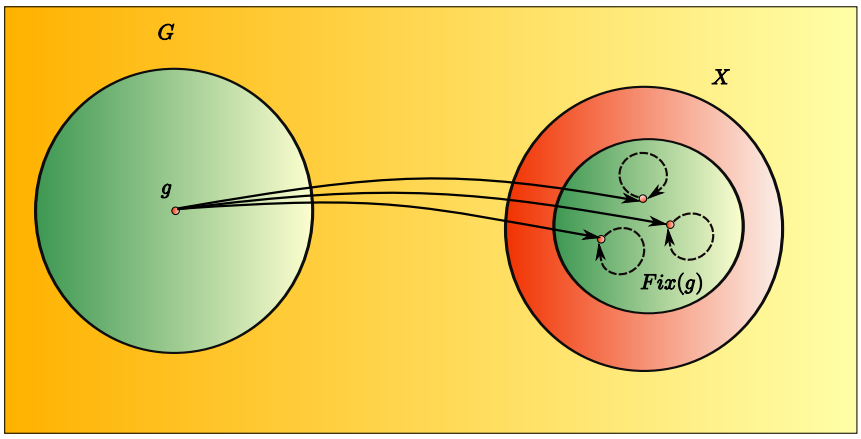

Fig. 26 - Fixateur

6.2 Scène V.2 - Propriétés

EURISTIDE : Ayant défini l'ensemble des objets relatifs aux actions de groupe, nous allons maintenant en observer les principales propriétés. La première propriété intéressante apparaît si l'on remarque que les orbites peuvent constituer des classes d'équivalence.

MATHINE : Ceci se traduit dans la proposition suivante.

Proposition **6.2.1**
Relation d'équivalence d'appartenance à une orbite
Soit X un ensemble. Soit G un groupe (cf. 4.1.5) agissant (cf. 6.1.1) sur X via une action θ. La relation sur X définie pour tout x, y appartenant à X par $x \sim y \Leftrightarrow y \in w(x)$ est une relation d'équivalence (cf. 2.1.4) sur X.

EURISTIDE : Autrement dit, si nous pouvons parler de relation d'équivalence, nous pouvons parler d'ensemble quotient. En d'autres termes, nous simplifions l'ensemble X en regardant les classes d'équivalence que sont les orbites, au lieu de regarder les éléments de X. En effet, puisque l'appartenance à une orbite est une relation d'équivalence, il s'ensuit que les classes d'équivalence de cette relation sont les orbites elles-mêmes. D'ailleurs, ceci nous permet de confirmer que les orbites constituent une partition de l'ensemble X.

BEATRIX : On pouvait s'y attendre, puisque tout élément est nécessairement dans une orbite (au pire, son orbite est constituée de cet élément seul s'il est invariant sous l'action de G). Par ailleurs, si

un élément $z \in X$ était l'image de deux actions g et g' sur deux éléments x et x' de X, alors on aurait $z = g.x = g'.x$ et par conséquent, en agissant par g^{-1} à gauche sur $g'.x'$, on obtiendrait $x = g^{-1}(g'.x')$. Donc x et x' seraient dans la même orbite. Ceci garantit donc que les orbites ne se recouvrent pas.

`EURISTIDE` : Prenons un exemple. X est l'ensemble des lettres $\{A, B, C, D, E, F\}$. Soit G le groupe $\{0, 1, 2, 3, 4, 5\}$, muni de la loi d'addition :

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

L'action de $g \in G$ sur une lettre de X fait passer à la g-ième lettre après celle-ci, en revenant de F à A lorsqu'on rencontre F dans le processus.

`BEATRIX` : J'écris la table de l'action du groupe comme suit :

	A	B	C	D	E	F
0	A	B	C	D	E	F
1	B	C	D	E	F	A
2	C	D	E	F	A	B
3	D	E	F	A	B	C
4	E	F	A	B	C	D
5	F	A	B	C	D	E

Il n'y a évidemment qu'un seule orbite, c'est $\{A, B, C, D, E, F\}$, c'est-à-dire l'ensemble X entièrement.

`EURISTIDE` : Un autre exemple, avec l'ensemble $\{A, B, C, D, E, F, G, H, I, J, K, L\}$. Cette fois, l'action fait correspondre à une lettre une autre lettre suivant la table ci-dessous :

	A	B	C	D	E	F	G	H	I	J	K	L
0	A	B	C	D	E	F	G	H	I	J	K	L
1	B	C	D	E	F	A	H	I	J	K	L	G
2	C	D	E	F	A	B	I	J	K	L	G	H
3	D	E	F	A	B	C	J	K	L	G	H	I
4	E	F	A	B	C	D	K	L	G	H	I	J
5	F	A	B	C	D	E	L	G	H	I	J	K

On trouve deux orbites, d'une part :

$$\{A, B, C, D, E, F\} \tag{311}$$

et, d'autre part :

$$\{G, H, I, J, K, L\} \tag{312}$$

`MATHINE` : Démontrons maintenant que les orbites sont bien des classes d'équivalence.

Démonstration :

1) Considérons la relation sur X :

$$x \sim y \Leftrightarrow y \in w(x). \tag{313}$$

a) Démontrons que la relation est réflexive.
On a :

$$x \in w(x), \tag{314}$$

donc $x \sim x$.
Donc la relation est réflexive.

b) Démontrons que la relation est symétrique.
Soit $y \in w(x)$. Alors, il existe $g \in G$ tel que :

$$y = g.x. \tag{315}$$

Considérons alors l'élément $g^{-1}.y$.
On a, par compatibilité de l'action avec la loi de groupe :

$$\begin{aligned} g^{-1}.y &= g^{-1}.(g.x) && (316)\\ &= (g^{-1}g).x && (317)\\ &= e.x && (318)\\ &= x. && (319) \end{aligned}$$

Donc, $x \in w(y)$.
Par conséquent, la relation est symétrique.

c) Démontrons que la relation est transitive.
Soit $y \in w(x)$ et soit $z \in w(y)$.
Alors, il existe $g \in G$ tel que :

$$y = g.x, \tag{320}$$

et il existe $g' \in G$ tel que :

$$z = g'.y. \tag{321}$$

Substituons l'expression de y dans cette deuxième égalité :

$$z = g'.(g.x) \tag{322}$$

et par compatibilité de l'action avec la loi de groupe :

$$z = (g'.g).x. \tag{323}$$

Donc $z \in w(x)$.
Par conséquent, la relation est transitive.

d) Donc la relation est une relation d'équivalence.

2) La classe d'équivalence de x pour cette relation est l'ensemble :

$$\overline{x} = \{y \in X; \quad y \in w(x)\}. \tag{324}$$

Donc :

$$\overline{x} = w(x). \tag{325}$$

Par conséquent, les classes d'équivalence sont bien les orbites des éléments de X.

C.Q.F.D.

EURISTIDE : Nous allons maintenant chercher la structure du stabilisateur.

BEATRIX : Hum... C'est un sous-ensemble du groupe G, et on a vu tout à l'heure qu'il contenait nécessairement l'élément neutre e. Donc, si structure il y a, je parierais bien que ce sera un sous-groupe.

MATHINE : Gagné. Voici la proposition correspondante.

Proposition **6.2.2**
Sous-groupe stabilisateur
Soit X un ensemble. Soit G un groupe (cf. 4.1.5) agissant (cf. 6.1.1) sur X via une action θ. Si x est élément de X, alors Stab(x) (cf. 6.1.4) est un sous-groupe (cf. 4.2.1) de G.

EURISTIDE : Le stabilisateur nous fait un peu penser au noyau d'un homomorphisme. Bien sûr, il n'est pas de même nature, mais disons que pour un élément x fixé, le stabilisateur est à l'action du groupe G, ce que le noyau est à l'homomorphisme.

BEATRIX : Oui, je comprends bien le parallèle. Le noyau d'un homomorphisme est le sous-groupe transformé en élément neutre ; le stabilisateur de x pour l'action de G est le sous-groupe qui laisse x invariant.

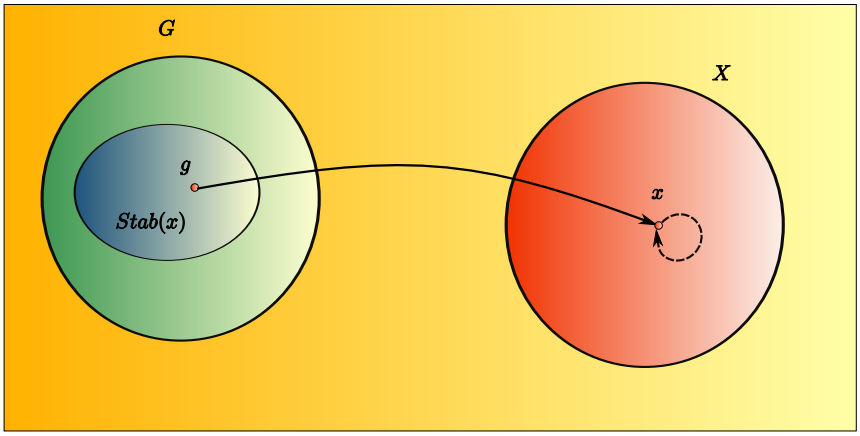

Fig. 27 - Stabilisateur

`MATHINE` : Voilà. Démontrons donc que ce stabilisateur est bien un sous-groupe.

Démonstration :

1) Soit e l'élément neutre de G.
   Alors :
$$e.x = x. \tag{326}$$
   Donc $e \in Stab(x)$.
2) Soit $g, g' \in Stab(x)$.
   Alors :
$$g.x = x \tag{327}$$
$$g'.x = x. \tag{328}$$
   Par conséquent, on peut écrire :
$$g^{'-1}.x = x. \tag{329}$$
   Donc :
$$g(g^{'-1}.x) = x, \tag{330}$$
   d'où :
$$(gg^{-1}).x = x. \tag{331}$$
   Donc $gg^{'-1} \in Stab(x)$.
3) Donc $Stab(x)$ est bien un sous-groupe de G.

C.Q.F.D.

EURISTIDE : Nous avions vu précédemment les sous-groupes conjugués. Je rappelle que ce sont des sous-groupes qui sont en relation par une multiplication à gauche et à droite ; autrement dit, H et K sont des sous-groupes conjugués de G s'il existe un élément $g \in G$ tel que :

$$gH = Kg. \tag{332}$$

En d'autres termes, les multiples à gauche de H par g sont exactement les multiples à droite de K par g. En voici une application.

MATHINE : Voici en effet une application de cette notion de sous-groupes conjugués dans le cadre des stabilisateurs d'une action.

Proposition **6.2.3**
Les stabilisateurs d'une même orbite sont conjugués
Soit X un ensemble. Soit G un groupe (cf. 4.1.5) agissant (cf. 6.1.1) sur X via une action θ. Si x et y sont des éléments de X d'une même orbite (cf. 6.1.5), alors $Stab(x)$ (cf. 6.1.4) et $Stab(y)$ sont des sous groupes (cf. 4.2.1) conjugués (cf. 5.4.2) de G.

EURISTIDE : Essayons de bien comprendre cette propriété. Puisque x et y sont dans la même orbite, il existe un élément $g \in G$ dont l'action sur x donne y.

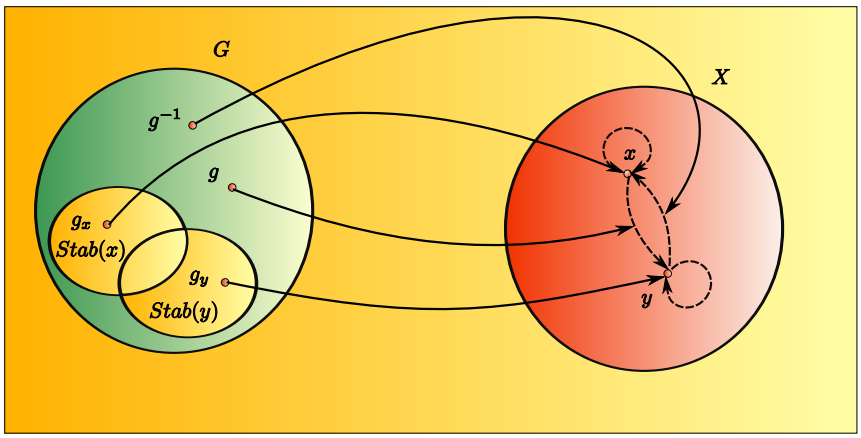

Fig. 28 - Stabilisateurs d'une même orbite conjugués

On comprend alors qu'en faisant agir d'abord g^{-1} sur y, on retrouve x. Puis en faisant agir un élément g_x de $Stab(x)$ sur x, on retrouve de nouveau x. Enfin, en faisant agir g sur x, on trouve y. C'est donc que nous pouvons reconstituer le stabilisateur de y par cette manipulation $g.h'.g^{-1}$ sur les éléments du stabilisateur de x. C'est donc qu'il sont conjugués.

`MATHINE` : Plus formellement, la démonstration donne ceci.

Démonstration :

Puisque x et y appartiennent à la même orbite, alors, il existe $g \in G$ tel que :

$$g.x = y. \tag{333}$$

Pour montrer l'égalité des ensembles $Stab(y)$ et $g.Stab(x).g^{-1}$, nous allons montrer l'inclusion réciproque de ces deux ensembles.

1) Considérons $h \in g.Stab(x).g^{-1}$.
   Alors, on peut écrire :

$$h = g.g_x.g^{-1}, \tag{334}$$

   où $g_x \in Stab(x)$.
   Calculons :

$$\begin{aligned} h.y &= g.g_x.g^{-1}.y && (335)\\ &= g.g_x.(g^{-1}.y) && (336)\\ &= g.g_x.x && (337)\\ &= g.x && (338)\\ &= h. && (339) \end{aligned}$$

   Donc, $h \in Stab(y)$.
   Donc $g.Stab(x).g^{-1} \subseteq Stab(y)$.
2) Inversement, soit $h \in Stab(y)$ quelconque.
   Considérons $h' = g^{-1}.h.g$.
   Alors :

$$h = g.h'.g^{-1}. \tag{340}$$

   Calculons :

$$\begin{aligned} h'.x &= g^{-1}.h.g.x && (341)\\ &= g^{-1}.h.(g.x) && (342)\\ &= g^{-1}.h.y. && (343) \end{aligned}$$

   Or, $h \in Stab(y)$, donc $h.y = y$.
   D'où :

$$\begin{aligned} h'.x &= g^{-1}.y && (344)\\ &= x. && (345) \end{aligned}$$

   Donc $h' \in Stab(x)$.
   Par conséquent, $h \in g.Stab(x).g^{-1}$.
   Donc, $Stab(y) \subset g.Stab(x).g^{-1}$.

3) Donc finalement :

$$Stab(y) = g.Stab(x).g^{-1}. \tag{346}$$

Donc, $Stab(x)$ et $Stab(y)$ sont conjugués.

C.Q.F.D.

EURISTIDE : Nous avons établi tout à l'heure un parallèle intuitif intéressant entre noyau d'un homomorphisme et stabilisateur d'un élément. On peut poursuivre ce parallèle et donner au stabilisateur le rôle du noyau, à l'action le rôle de l'homomorphisme et à l'orbite le rôle de l'image.

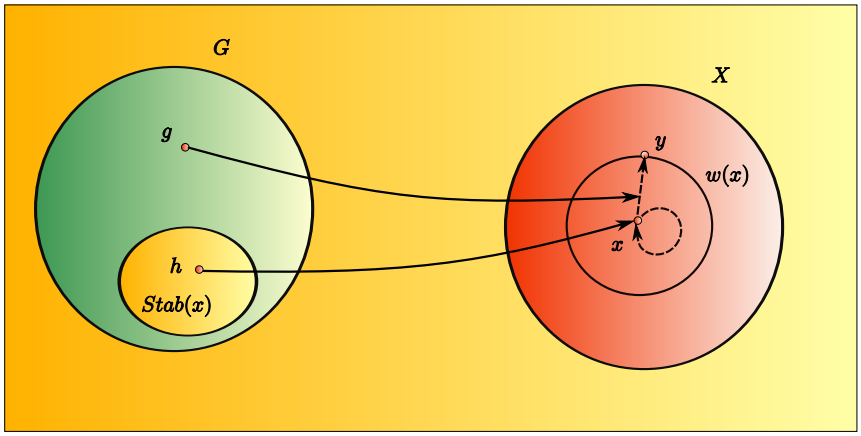

Fig. 29 - Orbite et quotient

BEATRIX : Je vois où vous voulez en venir. Comme nous l'avions fait pour les groupes quotients, nous pourrions tenter un passage au quotient par le stabilisateur, et mettre ainsi en évidence une bijection entre "l'image" (donc l'orbite) et l'ensemble quotient de G par le "noyau" (donc le stabilisateur).

MATHINE : C'est ce que nous allons faire dans la proposition suivante.

Proposition 6.2.4
Bijection entre l'orbite et le quotient par le stabilisateur
Soit X un ensemble. Soit G un groupe (cf. 4.1.5) agissant sur X via une action (cf. 6.1.1) θ. Soit $x \in X$. On a une bijection (cf. 4.3.5) entre $G/Stab(x)$ (cf. 6.1.4) et $w(x)$ (cf. 6.1.5).

EURISTIDE : Ainsi, par cette proposition $G/Stab(x)$ simplifie le groupe G pour placer dans une même classe les éléments qui sont identiques à un facteur multiplicatif près stabilisant x. On comprend bien que ceci revient à mettre dans une même classe tous les éléments de G qui produisent la même action sur l'élément x. Ce qui veut dire que chaque classe va produire une action différente sur x.

BEATRIX : Ca y est, je comprends. Donc, nous allons pouvoir faire correspondre point à point chaque classe $G/Stab(x)$ (l'ensemble quotient) à un élément distinct de l'orbite de x. C'est comme cela, je suppose, que la bijection va se construire.

MATHINE : C'est ce qui va se passer. En voici la démonstration.

Démonstration :

Pour démontrer cette proposition, nous allons considérer une application correctement choisie de $G/Stab(x)$ sur $w(x)$ et montrer tour à tour qu'elle est surjective et injective.

1) Considérons l'application f définie par :

$$\begin{array}{rccc} f: & G/Stab(x) & \longrightarrow & w(x) \\ & \overline{x} & \longmapsto & f(\overline{g}) = g.x. \end{array} \tag{347}$$

Il nous faut d'abord vérifier que nous bien le droit de définir une telle application, parce que nous avons choisi, pour cette fonction, un élément g arbitraire dans $\overline{g}$. Autrement dit, il faut vérifier que l'application f ne dépend pas du choix du représentant choisi dans $\overline{g}$.
Soit donc deux représentants g et g' de $\overline{g}$.
Alors, par définition de l'ensemble quotient, il existe $h \in Stab(x)$ tel que :

$$g' = gh. \tag{348}$$

Par conséquent :

$$\begin{aligned} f(\overline{g}) &= g'.x && (349)\\ &= gh.x && (350)\\ &= g(h.x) && (351)\\ &= g.x. && (352) \end{aligned}$$

Donc, $f(\overline{g})$ ne dépend pas du choix du représentant, et donc est bien définie.

2) Surjectivité :
Soit $y \in w(x)$. Alors, par définition, il existe $g \in G$ tel que :

$$y = g.x. \tag{353}$$

Par conséquent :

$$y = f(\overline{g}). \tag{354}$$

Donc f est bien surjective.

3) Injectivité :
Soit $\overline{g}$ et $\overline{h}$ éléments de $G/Stab(x)$ tels que :

$$f(\overline{g}) = f(\overline{h}). \tag{355}$$

Alors :

$$g.x = h.x. \tag{356}$$

Donc :

$$h^{-1}g.x = x. \tag{357}$$

Par conséquent, $h^{-1}g \in Stab(x)$.
Donc $\overline{h^{-1}g} = \overline{e}$, dans $G/Stab(x)$.
Or :

$$\overline{h^{-1}g} = \overline{h^{-1}}.\overline{g} \tag{358}$$

$$= \overline{h}^{-1}.\overline{g} \tag{359}$$

puisque la classe d'un inverse est bien égale à l'inverse de la classe, en considérant la loi induite par la loi de groupe dans $G/Stab(x)$. En effet, $\overline{h^{-1}} = \{x \in G; \exists y \in G, x = h^{-1}y\}$ et $\overline{h}^{-1} = \{x \in G; \exists y \in G, x = (hy)^{-1}\}$. Donc $\overline{h^{-1}} = \overline{h}^{-1}$. Donc :

$$\overline{h}^{-1}.\overline{g} = \overline{e}. \tag{360}$$

D'où :

$$\overline{g} = \overline{h}. \tag{361}$$

Donc, f est injective.

4) Donc finalement, f est bijective.

C.Q.F.D.

BEATRIX : Donc, si $G/Stab(x)$ et l'orbite de x sont en bijection, leurs cardinaux sont égaux, n'est-ce pas ?

MATHINE : C'est tout à fait exact, Béatrix, et c'est pourquoi nous allons pouvoir énoncer le corollaire suivant.

Proposition 6.2.5
Relation avec cardinaux du groupe, du stabilisateur et de l'orbite
Soit X un ensemble. Soit G un groupe (cf. 4.1.5) agissant sur X via une action (cf. 6.1.1) θ. Supposons que G est fini. Soit $x \in X$. Soit $Stab(x)$ son stabilisateur (cf. 6.1.4). Soit $w(x)$ son orbite (cf. 6.1.5). Alors :

$$\frac{|G|}{|Stab(x)|} = |w(x)| \tag{362}$$

EURISTIDE : Cette proposition est effectivement la conséquence très intuitive de la précédente, puisque l'existence de la bijection entre quotient $G/Stab(x)$ et l'orbite de x nous conduit à l'égalité des cardinaux correspondants.
Cette relation s'écrit également :

$$|G| = |w(x)||Stab(x)|, \tag{363}$$

et en particulier, il faut retenir que le cardinal de toute orbite divise celui du groupe G.

MATHINE : Voici la démonstration, qui est assez facile.

Démonstration :

D'après la proposition (cf. 6.2.4), il y a égalité des cardinaux :

$$|G/Stab(x)| = |w(x)|. \tag{364}$$

Or, d'après le théorème de Lagrange (cf. 5.1.1), $|G/Stab(x)|$ n'est rien d'autre que l'indice du sous-groupe $Stab(x)$ dans G :

$$[G : Stab(x)] = \frac{|G|}{|Stab(x)|} = |G/Stab(x)|. \tag{365}$$

D'où le résultat :

$$|w(x)| = \frac{|G|}{|Stab(x)|}. \tag{366}$$

C.Q.F.D.

EURISTIDE : Jusqu'à présent, nous nous sommes intéressés à un élément particulier $x \in X$, à son orbite et à son stabilisateur. Mathine va nous montrer maintenant comment nous pouvons généraliser.

MATHINE : En effet, pour généraliser, nous allons devoir considérer les orbites de X sous l'action de G, qui constituent une partition de X. Alors nous pourrons facilement faire la somme des cardinaux des sous-ensembles disjoints que constituent les orbites, et obtenir la proposition suivante.

Proposition **6.2.6**
Somme des cardinaux des orbites
Soit X un ensemble. Soit G un groupe (cf. 4.1.5) fini agissant (cf. 6.1.1) sur X via une action θ. Soit $\{x_i; i = 1, \ldots, n\}$ un sous ensemble d'éléments de X tel que $\{w(x_i); i = 1, \ldots, n\}$ est une partition (cf. 2.1.7) de X. Alors :

$$|X| = \sum_{i=1}^{n} |w(x_i)| = |G| \sum_{i=1}^{n} \left(|Stab(x_i)|\right)^{-1}. \tag{367}$$

EURISTIDE : Nous avons vu que la relation "est dans l'orbite de" est une relation d'équivalence sur X. C'est ce qui nous a permis de déduire que les orbites constituaient une partition de l'ensemble X.

BEATRIX : Alors, en effet, la proposition se déduit facilement des deux précédentes. Dans la mesure où nous avons constitué une partition de X avec les orbites, nous appliquons les propriétés précédentes à chacune des orbites, et le partitionnement de X nous permet de conclure.

MATHINE : C'est bien comme cela que nous allons démontrer cette proposition.

Démonstration :

Pour chaque x_i, d'après la proposition précédente, nous avons :

$$\frac{|G|}{|Stab(x_i)|} = |w(x_i)|. \tag{368}$$

Or, puisque les $w(x_i)$ constituent une partition de X, nous avons :

$$|X| = \sum_{i=1}^{n} |w(x_i)|. \tag{369}$$

Par conséquent, nous pouvons écrire :

$$|X| = \sum_{i=1}^{n} \frac{|G|}{|Stab(x_i)|} \tag{370}$$

$$= |G| \sum_{i=1}^{n} \frac{1}{|Stab(x_i)|}. \tag{371}$$

C.Q.F.D.

EURISTIDE : Le théorème suivant va nous permettre d'obtenir le nombre d'orbites.

MATHINE : Voici la formule de la moyenne qui permet de déterminer le nombre d'orbites dans X.

Théorème **6.2.1 (Formule de la moyenne)** *Soit X un ensemble. Soit G un groupe fini agissant sur X via une action θ. Soit n le nombre d'orbites distinctes de l'action. Alors on a :*

$$n = \frac{1}{|G|} \sum_{g \in G} |X^g| \,. \tag{372}$$

X^g est le fixateur de g (cf. 6.1.6).

EURISTIDE : Cette formule s'explique comme suit. On prend chaque représentant d'une orbite distincte de l'action. On considère alors le fixateur de ce représentant : c'est l'ensemble des éléments de X sur lesquels ce représentant n'a pas d'action.
Intuitivement, puisqu'on parle en fait de la même propriété à la base, il y a autant de fixateurs dans X quand on parcourt les éléments de G, qu'il y a de stabilisateurs dans G quand on parcourt les éléments de X.
Or, nous savons que le cardinal du stabilisateur est égal au rapport du cardinal de G sur le cardinal de l'orbite de cet élément. En faisant la somme de ces rapports sur tous les stabilisateurs des éléments de X, on fait ainsi la somme de ces rapports pour un représentant de chaque orbite multiplié par la somme pour tous les éléments de l'orbite.

En procédant ainsi, on compte autant de fois le cardinal de G qu'il y a d'orbites distinctes. c'est ce qui nous conduit au résultat annoncé.

`MATHINE` : La démonstration s'appuie sur le raisonnement fait par Euristide.

Démonstration :

1) Considérons l'égalité, pour $g \in G$ et $x \in X$:

$$g.x = x. \tag{373}$$

Il y a deux façons d'interpréter cette égalité :
- $x \in Fix(g)$, où $Fix(g)$ est le fixateur de g, c'est-à-dire l'ensemble des éléments de X invariants par g.
- $g \in Stab(x)$, où $Stab(x)$ est le stabilisateur de x, c'est-à-dire l'ensemble des éléments de G qui laissent x invariant.

Donc, cela revient au même de compter :
- la somme des cardinaux des fixateurs de g, pour tous les éléments g de G,
- la somme des cardinaux des stabilisateurs de x, pour tous les éléments x de X.

Autrement dit :

$$\sum_{g\in G} |Fix(g)| = \sum_{x\in X} |Stab(x)|. \tag{374}$$

2) On note également :

$$Fix(g) = X^g. \tag{375}$$

Donc, nous pouvons noter, pour la suite :

$$\sum_{g\in G} |X^g| = \sum_{x\in X} |Stab(x)|. \tag{376}$$

3) Mais l'ensemble des $x \in X$ peut être considéré comme l'ensemble des $x \in w(x_i)$ où les $w(x_i)$ constituent la partition de X crée par les orbites des éléments de X sous l'action de G. Supposons qu'il y ait n orbites. Alors :

$$\sum_{g\in G} |X^g| = \sum_{i=1}^{n} \sum_{x\in w(x_i)} |Stab(x_i)|. \tag{377}$$

Or, nous savons que :

$$|w(x_i)| = \frac{|G|}{|Stab(x_i)|}, \tag{378}$$

donc :

$$|Stab(x_i)| = \frac{|G|}{|w(x_i)|}, \tag{379}$$

d'où :

$$\sum_{g\in G} |X^g| = \sum_{i=1}^{n} \sum_{x\in w(x_i)} \frac{|G|}{|w(x_i)|} \tag{380}$$

$$= |G| \sum_{i=1}^{n} \sum_{x\in w(x_i)} \frac{1}{|w(x_i)|}. \tag{381}$$

4) Mais le terme $\sum_{x\in w(x_i)} \frac{1}{|w(x_i)|}$ fait la somme $|w(x_i)|$ fois du terme $\frac{1}{|w(x_i)|}$. Donc ce terme vaut 1. Et par conséquent :

$$\sum_{g\in G} |X^g| = |G| \sum_{i=1}^{n} 1 \quad (382)$$

$$= |G|n. \quad (383)$$

5) D'où le résultat :

$$n = \frac{1}{|G|} \sum_{g\in X} |X^g|. \quad (384)$$

C.Q.F.D.

7 Acte VI - Les groupes et les nombres premiers

7.1 Scène VI.1 - Théorème de Cauchy

EURISTIDE : Nous allons maintenant nous intéresser à une série de propriétés concernant les groupes et leur relation avec les nombres premiers. C'est ce qui nous permettra d'établir un pont entre la théorie des groupes et la théorie des nombres classique.

MATHINE : Nous allons en particulier commencer par énoncer le théorème de Cauchy.

Théorème 7.1.1 (Théorème de Cauchy) *Soit $(G,.)$ un groupe (cf. 4.1.5) fini (cf. 4.4.4). Soit p un diviseur premier de l'ordre de G. Alors il existe un élément d'ordre (cf. 4.4.7) p dans G.*

EURISTIDE : Considérons par exemple le groupe $\{0,1,2,3,4,5\}$, muni de la loi $\oplus$ définie par la table :

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Ce groupe est d'ordre 6. Les diviseurs premiers de 6 sont 2 et 3.

BEATRIX : Et 2 est d'ordre 3, et 3 est d'ordre 2, effectivement, puisque $2 \oplus 2 \oplus 2 = 0$ et $3 \oplus 3 = 0$. Ca marche ici, mais ce que je ne comprends pas bien, c'est pourquoi cette propriété est vraie en général.

EURISTIDE : Pour bien comprendre ce qui se passe, nous allons analyser les p-uplets d'éléments dont le produit vaut e :

$$x_1 \dots x_p = e. \tag{385}$$

Il y a $|G|^{p-1}$ exemplaires de tels p-uplets, puisqu'il suffit de choisir arbitraitement $x_1, \dots, x_{p-1}$ (c'est-à-dire $|G|^{p-1}$ possibilités) et alors x_p sera déduit par le calcul suivant :

$$x_p = (x_1 \dots x_{p-1})^{-1}. \tag{386}$$

Dans ces p-uplets, on peut distinguer deux grandes catégories :

a) Les p-uplets où tous les x_i sont égaux, donc tels que, par exemple :

$$x_1^p = e. \tag{387}$$

b) Les autres p-uplets.

Dans la catégorie b), nous pouvons réunir dans une même classe tous les p-uplets qui se déduisent les uns des autres par permutation circulaire des x_i. Chacune de ces classes possède nécessairement p éléments, puisqu'il y a p permutations circulaires des x_i possibles. Donc, l'ensemble des éléments de la catégorie b) peut être rangé sous forme de classes de p éléments. Par conséquent, son cardinal est divisible par p.
Le nombre total de p-uplets est $|G|^{p-1}$, donc également divisible par p, puisque p divise l'ordre de G.
Par conséquent, le nombre de p-uplets de la catégorie a) qui est égal au nombre total de p-uplets moins ceux de la catégorie b) est divisible par p. Donc, en dehors de $(e, \dots, e)$ qui est lui-même dans la catégorie a), il y a au moins $p-1$ autres éléments.

BEATRIX : Ce n'est pas simple, mais c'est astucieux. En résumé, le nombre des p-uplets dont le produit est e est divisible par p, et le nombre de p-uplets dont les éléments ne sont pas tous égaux est également divisible par p. Donc, le nombre d'éléments x tels que $x^p = e$ est aussi divisible par p.

EURISTIDE : Voilà, c'est cela.

MATHINE : Pour le démontrer de façon élégante, nous allons utiliser les actions de groupe.

Démonstration :

1) Considérons l'ensemble X défini comme suit :

$$X = \{(x_1, \dots, x_p) \in G^p; \quad x_1 \dots x_p = e\}. \tag{388}$$

Considérons la permutation circulaire :

$$c = (1, 2, \dots, p) \tag{389}$$

qui à 1 fait correspondre 2, à i fait correspondre $i+1$, et à p fait correspondre 1.
Considérons le groupe $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{p-1}\}$, dont la loi est définie par :

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\ldots$	$\overline{p-1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\ldots$	$\overline{p-1}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\ldots$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\ldots$	$\overline{1}$
$\vdots$	$\ldots$	$\ldots$	$\ldots$	$\vdots$	$\ldots$
$\overline{p-1}$	$\overline{p-1}$	$\overline{0}$	$\overline{1}$	$\ldots$	$\overline{p-2}$

BEATRIX : Ah oui ! C'est l'équivalent, généralisé pour p, du groupe que nous avons défini $\{0, 1, 2, 3, 4, 5\}$ à plusieurs reprises.

EURISTIDE : Il faut noter que ce groupe $\mathbb{Z}/p\mathbb{Z}$ est un groupe quotient construit comme le quotient du groupe $\mathbb{Z}$ par le sous-groupe $p\mathbb{Z}$ des entiers multiples de p dans $\mathbb{Z}$. Par ce passage au quotient, nous constituons la classe des multiples de p, puis la classe des multiples de p auxquels on ajoute 1, puis la classe des multiples de p auxquels on ajoute 2, etc., jusqu'à la classe des multiples de p auxquels on ajoute $p-1$. Le groupe quotient $\mathbb{Z}/p\mathbb{Z}$ contient donc p classes.

MATHINE : Alors, nous définissons une action de $\mathbb{Z}/p\mathbb{Z}$ sur G^p en posant :

$$\forall \overline{k} \in \mathbb{Z}/p\mathbb{Z}, \forall x = (x_1, \ldots, x_p) \in G^p, \quad \overline{k}.x = (x_{c^k(1)}, \ldots, x_{c^k(p)}), \tag{390}$$

où c^k représente l'exécution de la permutation circulaire c, k fois de suite.
Cette loi est bien une action de groupe, puisque :

$$\begin{aligned} \overline{0}.x &= (x_{c^0(1)}, \ldots, c_{c^0(p)}) && (391)\\ &= (x_1, \ldots, x_p) && (392)\\ &= x, && (393) \end{aligned}$$

donc $\overline{0}$ est invariant pour tout élément de X ; et si $\overline{k}$ et $\overline{l}$ sont des éléments de $\mathbb{Z}/p\mathbb{Z}$, on a :

$$\begin{aligned} \overline{k}.(\overline{l}.x) &= \overline{k}(x_{c^l(1)}, \ldots, x_{c^l(p)}) && (394)\\ &= (x_{c^{k+l}(1)}, \ldots, x_{c^{k+l}(p)}) && (395)\\ &= (\overline{k} \oplus \overline{l}).x. && (396) \end{aligned}$$

Donc, l'action est bien compatible avec la loi de groupe dans $\mathbb{Z}/p\mathbb{Z}$.
D'autre part, X est une partie stable pour l'action, puisque si $x \in X$:

$$\overline{1}.x = (x_2, \ldots, x_p, x_1), \tag{397}$$

et :

$$\begin{aligned} x_2 \ldots x_p x_1 &= (x_1^{-1} x_1) x_2 \ldots x_p x_1 && (398)\\ &= x_1^{-1}(x_1 x_2 \ldots x_p) x_1 && (399)\\ &= x_1^{-1} e x_1 && (400)\\ &= x_1^{-1} x_1 && (401)\\ &= e. && (402) \end{aligned}$$

Donc $\overline{1}.x \in X$.
Procédons par récurrence à partir de ce point. Supposons la propriété $\overline{k}.x \in X$ vérifiée pour $\overline{k}$. Alors :

$$\overline{k+1}.x = \overline{1}.\overline{k}.x \tag{403}$$

Or, $\overline{k}.x \in X$ par hypothèse de récurrence, donc $1.(\overline{k}.x) \in X$.
Donc X est bien stable pour l'action.

2) Ayant défini une action sur X, nous allons étudier le cardinal de X, maintenant.
Les éléments de X sont définis en choisissant arbitraitement $x_1, x_2, \ldots, x_{p-1}$. Puis x_p est déterminé par :

$$x_p = (x_1 x_2 \ldots x_{p-1})^{-1}. \tag{404}$$

Il y a $|G|^{p-1}$ façons de choisir les $x_1, \ldots, x_{p-1}$, donc :

$$|X| = |G|^{p-1}. \tag{405}$$

3) Considérons les éléments de X dont l'orbite est ponctuelle. L'orbite de $x \in X$ est ponctuelle si et seulement si :

$$\overline{1}.x = (x_2, \ldots, x_p, x_1) = x, \tag{406}$$

ce qui est équivalent à :

$$x_1 = x_2 = \ldots = x_p. \tag{407}$$

Donc, les orbites ponctuelles correspondent aux éléments x_1 de G tels que :

$$x_1^p = e. \tag{408}$$

Donc, ces orbites ponctuelles correspondent aux éléments de G dont l'ordre divise p. Comme p est premier, ce sont soit e (d'ordre 1), soit les éléments d'ordre p.
Notons s le nombre d'orbites ponctuelles dans X.

4) Soit k le nombre total d'orbites dans X. Comme $\mathbb{Z}/p\mathbb{Z}$ agit sur X, le cardinal d'une orbite non ponctuelle divise $|\mathbb{Z}/p\mathbb{Z}| = p$.
Donc ce cardinal est p, puisqu'il n'est pas égal à 1 par définition d'une orbite non ponctuelle, et puisque p est premier.

5) Par conséquent :

$$|X| = |G|^{p-1} = s + (k-s)p = n^{p-1}, \tag{409}$$

où n est le cardinal de G.
Par hypothèse $p|n$
Par conséquent, $p|s$.
or, $(e, \ldots, e)$ constitue un exemple d'orbite ponctuelle. Donc, il existe au moins $(p-1)$ éléments d'ordre p dans G.

C.Q.F.D.

7.2 Scène VI.2 - Théorèmes de Sylow

EURISTIDE : Nous allons maintenant poursuivre notre investigation de la relation entre groupes et nombres premiers en regardant les p-groupes et les p-Sylow.

MATHINE : Commençons par définir un p-groupe.

Définition **7.2.1**
p-groupe
On dit que le groupe (cf. 4.1.5) fini (cf. 4.4.4) $(G, .)$ est un p-groupe si p est premier et si le cardinal (cf. 4.4.3) de G est une puissance de p.

BEATRIX : Donc, si je comprends bien, les p-groupes sont des groupes de cardinal p^n où p est premier.

EURISTIDE : Oui. Et comme l'ordre des éléments doit diviser l'ordre du groupe, il en découle que les éléments d'un p-groupe sont d'ordre p^k où $k \in \mathbb{N}$.

MATHINE : Nous allons maintenant nous intéresser au cardinal d'un ensemble X qui subit l'action d'un p-groupe. La particularité du cardinal d'un p-groupe va imposer une contrainte sur le cardinal de l'ensemble X.

Proposition **7.2.1**
Cardinal d'un ensemble avec action d'un p-groupe
Soit G un p-groupe (cf. 7.2.1) agissant (cf. 6.1.1) sur un ensemble X. Soit X^G le fixateur (cf. 6.1.6) de G, c'est-à-dire l'ensemble des éléments de X dont l'orbite (cf. 6.1.5) est constituée d'un unique point. Alors on a :

$$|X| \equiv \left|X^G\right| \pmod{p}. \tag{410}$$

EURISTIDE : Pour comprendre cette propriété, il faut considérer que X est partitionné par X^G (ensemble des éléments dont l'orbite est ponctuelle) et un certain nombre d'orbites non ponctuelles $w(x_i)$.

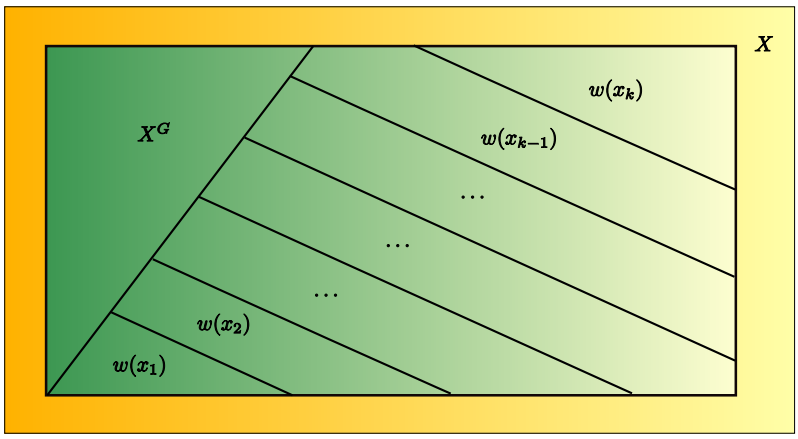

Fig. 30 - Partitionnement orbites ponctuelles

Donc le cardinal de X est la somme du cardinal de X^G et des cardinaux des orbites $w(x_i)$.
Or nous savons que le cardinal de toute orbite divise celui de G.

`BEATRIX` : Et G est un p-groupe, donc son cardinal est de la forme p^n.

`EURISTIDE` : Et voilà. Et donc le cardinal de toute orbite est une puissance de p.
En résumé, nous avons :

$$|w(x_i)| \equiv 0 \pmod{p}, \tag{411}$$

et :

$$|X| = \sum_{i=1}^{k} |w(x_1)| + |X^G|. \tag{412}$$

Par conséquent, $|X|$ et $|X^G|$ ont même reste dans la division par p, ce qui conduit au résultat.

`MATHINE` : Voici la démonstration, conforme à votre analyse.

Démonstration :

1) Partitionnons l'ensemble X au moyen des orbites de l'action du p-groupe G. Ceci a un sens, puisque les orbites d'une action d'un groupe partitionnent l'ensemble cible de l'action de groupe. Nous distinguons parmi ces orbites, celles qui sont ponctuelles et celles qui ne le sont pas.
La réunion des orbites ponctuelles est l'ensemble des éléments invariants sous l'action des éléments de G. C'est donc X^G, le fixateur de G.

Soit $(w(x_i))_{i=1,\dots,k}$ l'ensemble des orbites non ponctuelles complétant le partitionnement de X.
Alors :

$$|X| = |X^G| + \sum_{i=1}^{k} |w(x_i)|. \tag{413}$$

2) Or, le cardinal de toute orbite divise celui de G.
De plus :

$$|G| = p^n, \tag{414}$$

donc :

$$\forall i = 1, \dots, k, \quad |w(x_i)||p. \tag{415}$$

Donc :

$$\sum_{i=1}^{k} |w(x_i)| \equiv 0 \pmod{p}, \tag{416}$$

d'où :

$$|X| - |X^G| \equiv 0 \pmod{p}, \tag{417}$$

et finalement :

$$|X| \equiv |X^G| \pmod{p}. \tag{418}$$

C.Q.F.D.

EURISTIDE : Nous allons maintenant élargir le champ des p-groupes, en considérant les p-Sylow, qui sont des p-groupes particuliers.

MATHINE : En effet. Voici la définition d'un p-Sylow.

Définition **7.2.2**
p-Sylow
Soit G un groupe (cf. 4.1.5) de cardinal (cf. 4.4.3) $n = p^\alpha.m$ avec p premier et p ne divisant pas m. On dit que le sous groupe (cf. 4.2.1) H de G est un p-Sylow de G si $|H| = p^\alpha$.

EURISTIDE : Le p-Sylow est en quelque sorte le plus grand sous-groupe de G qui soit un p-groupe.

MATHINE : Pour analyser les propriétés de ces p-Sylow, nous allons commencer par démontrer un lemme qui nous sera utile par la suite.

Lemme **7.2.1**
Lemme pour les théorèmes de Sylow
Soit G un groupe (cf. 4.1.5) de cardinal (cf. 4.4.3) n. Soit p un diviseur premier de n, tel que $n = p^\alpha.m$, et p ne divisant pas m. Soit H un sous-groupe (cf. 4.2.1) de G et S un p-Sylow (cf. 7.2.2) de G. Alors il existe g dans G tel que $g.S.g^{-1} \cap H$ soit un p-sylow de H.

EURISTIDE : Ce lemme, qui est assez sophistiqué, nous indique que pour un sous-groupe H donné, il existe un sous-groupe de G conjugué au p-Sylow dont l'intersection à H est également un p-Sylow.

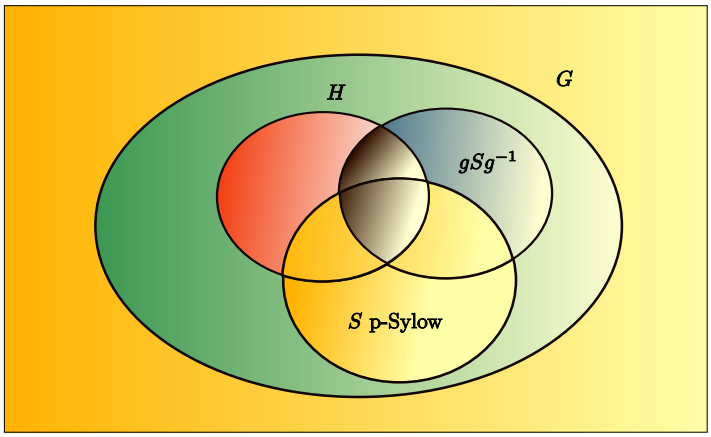

Fig. 31 - Intersection p-Sylow

Pour démontrer ce théorème, nous allons considérer le quotient de G par S, et faire agir G, puis H sur G/S.

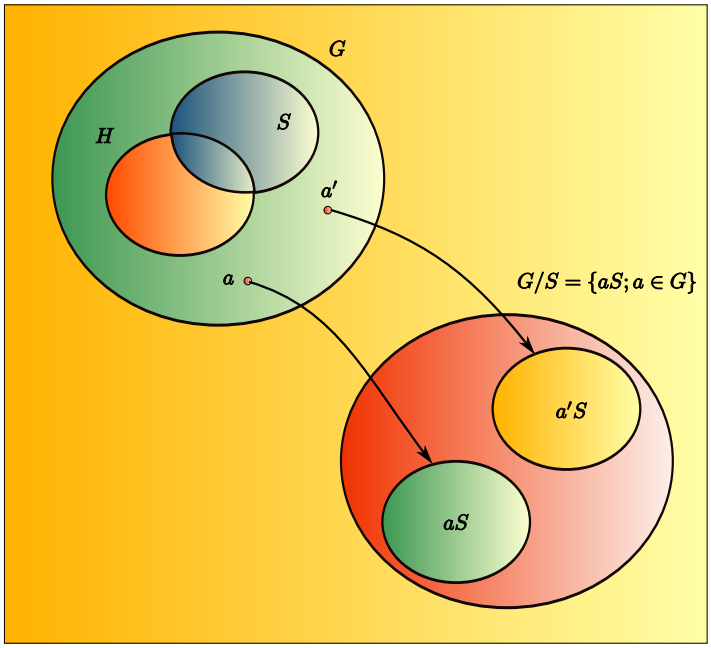

Fig. 32 - Action sur quotient d'un p-Sylow

La démonstration se fera en sept étapes : d'abord, nous identifions que les aSa^{-1} sont les stabilisateurs des éléments aS de G/S par l'action de G. Donc les $aSa^{-1} \cap H$ sont les stabilisateurs des éléments aS de G/S par l'action induite de H. Ensuite, on sait que $|S| = p^{\alpha}$, donc $|aSa^{-1}| = p^{\alpha}$ également, puisque c'est un sous-groupe conjugué. Puis, nous savons que le sous-groupe H de G a pour cardinal $|H| = m'.p^{\alpha'}$, avec $m'|m$ et $\alpha' \leq \alpha$, puisque $|H|$ divise $|G|$ d'après le théorème de Lagrange. Donc $|aSa^{-1} \cap H|$ divise $|S| = p^{\alpha}$ et $|H| = m'.p^{\alpha'}$. Donc $|aSa^{-1} \cap H|$ est de la forme $p^{\alpha''}$ où $\alpha'' \leq \alpha'$. Nous avons vu que les orbites des aS sous l'action de H constituent une partition de G/S. Or $|G/S| = m.p^{\alpha}/p^{\alpha} = m$. Donc p ne doit pas diviser $|G/S|$. Par ailleurs, nous savons que le cardinal d'une orbite sous l'action de H d'un aS est le rapport de $|H|$ au cardinal du stabilisateur de aS, c'est-à-dire que c'est :

$$|w(aS)| = \frac{|H|}{|aSa^{-1} \cap H|} = \frac{m'.p^{\alpha'}}{p^{\alpha''}}. \tag{419}$$

Donc, il est nécessaire que pour l'un des $w(aS)$, on ait $\alpha'' = \alpha'$, afin que p ne divise pas $|w(aS)|$, afin que p ne divise pas le cardinal de toutes les orbites et donc celui de G/H qui en est la somme.

`MATHINE` : Voici donc la démonstration précise, s'appuyant sur la construction d'Euristide.

Démonstration :

1) Nous considérons le quotient G/S. C'est l'ensemble des classes à gauche aS lorsque a parcourt G.
On peut considérer l'action de G sur G/S, par translation à gauche :

$$g.(aS) = (ga).S. \tag{420}$$

2) Montrons que $Stab(aS) = aSa^{-1}$.
Intéressons-nous au stabilisateur d'un élément aS.
Soit $g \in Stab(aS)$. Alors g est tel que :

$$g.aS = aS, \tag{421}$$

donc :

$$(ga).S = aS, \tag{422}$$

donc $ga \in aS$, ce qui équivaut à :

$$g \in aSa^{-1}. \tag{423}$$

Inversement, si $g \in aSa^{-1}$, alors il existe $s \in S$ tel que :

$$g = asa^{-1}. \tag{424}$$

Alors, soit t quelconque élément de S.

$$\begin{aligned} (ga)t &= g.at && (425)\\ &= asa^{-1}.at && (426)\\ &= ast. && (427) \end{aligned}$$

Donc :

$$(ga)t \in aS. \tag{428}$$

Donc $g.aS \subseteq aS$.
Inversement, soit t quelconque élément de S.

$$\begin{aligned} at &= asa^{-1}as^{-1}a^{-1}at && (429)\\ &= gas^{-1}a^{-1}at && (430)\\ &= gas^{-1}t. && (431) \end{aligned}$$

Donc :

$$at \in g.aS. \tag{432}$$

Donc $aS \subseteq g.aS$.
D'où finalement :

$$aS = g.aS. \tag{433}$$

Donc $g \in Stab(aS)$.
Finalement, nous avons démontré que :

$$Stab(aS) = aSa^{-1}. \tag{434}$$

3) Stabilisateur pour l'action de H.
L'action de G sur G/S induit sur H une action de H sur G/S, dont le stabilisateur est par conséquent de la forme $aSa^{-1} \cap H$.

4) Cardinal de $aSa^{-1} \cap H$.
S est un p-Sylow de G, donc $|S| = p^\alpha$.
aSa^{-1} est un sous-groupe de G, conjugué de S, donc il a même cardinal :

$$|aSa^{-1}| = p^\alpha. \tag{435}$$

H est un sous-groupe de G, donc son cardinal divise celui de G. Donc, il existe $m' \in \mathbb{N}$ tel que $m'|m$ et $\alpha' \in \mathbb{N}$ tel que $\alpha' \leq \alpha$, tels que :

$$|H| = m' p^{\alpha'}. \tag{436}$$

$aSa^{-1} \cap H$ est un sous-groupe de aSa^{-1}, donc son cardinal divise celui de aSa^{-1}, et par conséquent il existe $\alpha'' \in \mathbb{N}$ tel que $\alpha'' \leq \alpha'$ et tel que :

$$|aSa^{-1} \cap H| = p^{\alpha''}. \tag{437}$$

5) Orbites des classes de G/S sous l'action de H.
H définit une action sur G/S. Donc les orbites des éléments aS de G/H forment une partition de G/S.
Or :

$$|G/S| = \frac{|G|}{|S|} = \frac{mp^\alpha}{p^\alpha} = m. \tag{438}$$

Donc p ne divise pas $|G/S|$.
Par ailleurs, le cardinal d'une orbite sous l'action de H, d'un élément aS de G/S, est :

$$\begin{aligned} |w(aS)| &= \frac{|H|}{|Stab(aS)|} && (439)\\ &= \frac{|H|}{|aSa^{-1} \cap H|} && (440)\\ &= \frac{m'.p^{\alpha'}}{p^{\alpha''}} && (441)\\ &= m' p^{\alpha' - \alpha''}. && (442) \end{aligned}$$

6) Démontrons par l'absurde qu'il existe un a tel que $\alpha' = \alpha''$.
α'' dépend a priori du choix de a. Notons le α''_a.
Procédons par une démonstration par l'absurde.
Supposons que tous les α''_a soient tels que :

$$\forall a \in G, \alpha''_a < \alpha'. \tag{443}$$

Alors :

$$\forall a \in G, \quad p||w(aS)|. \tag{444}$$

Par conséquent, p divise le cardinal de toutes les orbites. Or ces orbites constituent une partition de G/S, donc p divise le cardinal de G/S.
C'est contradictoire avec ce que nous avons vu en 5).
Par conséquent, il existe $a \in G$ tel que :

$$\alpha''_a = \alpha'. \tag{445}$$

7) Par conséquent, nous avons la situation suivante, pour un tel a :

$$\begin{aligned} |H| &= m'.p^{\alpha'} && (446)\\ |aSa^{-1} \cap H| &= p^{\alpha'}. && (447) \end{aligned}$$

Donc $aSa^{-1} \cap H$ est un p-Sylow de H.

C.Q.F.D.

BEATRIX : Je trouve cette démonstration très astucieuse.

EURISTIDE : Ce lemme va nous être très utile dans les démonstrations des théorèmes de Sylow, pour mettre en évidence les propriétés de conjugaison.

MATHINE : Voici donc le premier théorème de Sylow.

Théorème **7.2.1 (Premier théorème de Sylow)** *Si G est un groupe (cf. 4.1.5) de cardinal (cf. 4.4.3) n et que n vérifie $n = p^{\alpha}.m$ avec p premier et p ne divisant pas m, alors G possède un p-Sylow (cf. 7.2.2).*

BEATRIX : On peut toujours décomposer un entier qui n'est pas une puissance pure d'un nombre premier, sous la forme $p^{\alpha}.m$. Donc, je pense en effet que tout groupe qui n'est pas un p-groupe possède un p-Sylow.

EURISTIDE : Oui, c'est bien la signification de ce premier théorème de Sylow.

MATHINE : Pour démontrer ce premier théorème de Sylow, nous allons avoir besoin d'un résultat de combinatoire particulier.

Lemme **7.2.2**
Propriété combinatoire
Soit p un nombre premier, $n \in \mathbb{N}^*$ et $s \in \mathbb{N}^*$ tels que $p \nmid s$. Alors, pour tout $1 \leq r \leq n$:

$$\left(\begin{array}{c} sp^n \\ p^r \end{array} \right) = \lambda p^{n-r}, \tag{448}$$

avec $\lambda \in \mathbb{N}^*$ tel que $p \nmid \lambda$.

Démonstration :

La démonstration se fait simplement par le calcul :

$$\left(\begin{array}{c} sp^n \\ p^r \end{array} \right) = \frac{(sp^n)!}{(p^r)!(sp^n - p^r)!} \tag{449}$$

$$= \frac{sp^n}{p^r}.\frac{sp^n - 1}{1}.\frac{sp^n - 2}{2} \cdots \frac{sp^n - (p^r - 1)}{p^r - 1}. \tag{450}$$

Pour tout k tel que $1 \leq k < p^r$, on peut écrire :

$$k = qp^{\alpha}, \tag{451}$$

avec $0 \leq \alpha < r$ et $p \nmid q$, donc :

$$\frac{sp^n - k}{k} = \frac{sp^{n-\alpha} - q}{q}, \tag{452}$$

avec $n - \alpha \geq 1$ et $p \nmid q$.
Par conséquent :

$$p \nmid q \tag{453}$$
$$p \nmid (sp^{n-\alpha} - q). \tag{454}$$

Donc, dans l'expression :

$$\frac{sp^n}{p^r} \cdot \frac{sp^n - 1}{1} \cdot \frac{sp^n - 2}{2} \cdots \frac{sp^n - (p^r - 1)}{p^r - 1}, \tag{455}$$

toutes les fractions à partir de la deuxième s'écrivent comme quotient de deux entiers que p ne divise pas.
Donc :

$$\left(\begin{array}{c} sp^n \\ p^r \end{array} \right) = \frac{xp^{n-r}}{y}, \tag{456}$$

où $p \nmid x$ et $p \nmid y$.
Or $\left(\begin{array}{c} sp^n \\ p^r \end{array} \right)$ est un entier. Donc $y|(xp^{n-r})$.
Or $p \nmid y$, donc $(p, y) = 1$, et par conséquent $y|x$.
Soit $\lambda = \frac{x}{y}$. Alors :

$$\left(\begin{array}{c} sp^n \\ p^r \end{array} \right) = \lambda p^{n-r}, \tag{457}$$

et $p \nmid \lambda$.

C.Q.F.D.

Nous pouvons maintenant démontrer le premier théorème de Sylow.

Démonstration :

Soit $r \in [1, n]$.

1) Soit $\mathcal{P}_r$ l'ensemble des sous-ensembles de G de cardinal p^r.
Nous savons que, pour tout $g \in G$, et pour tout sous-ensemble A de G :

$$|gA| = |A|. \tag{458}$$

Donc, en faisant opérer G par multiplication à gauche sur $\mathcal{P}_r$, nous obtenons toujours des éléments de $\mathcal{P}_r$.
Donc G opère bien sur $\mathcal{P}_r$.

2) Choisissons une famille $(A_i)_{i \leq i \leq l}$ de représentants des orbites distinctes de $\mathcal{P}_r$.
Or :

$$|w(A_i)| = \frac{|G|}{|Stab(A_i)|}. \tag{459}$$

Donc :

$$|\mathcal{P}_r| = \sum_{i=1}^{l} \frac{|G|}{|A_i^G|}. \tag{460}$$

Supposons que p^{n-r+1} divise $\frac{|G|}{|A_i^G|}$ pour tout i, alors p^{n-r+1} diviserait également $|\mathcal{P}_r|$.
Or $|\mathcal{P}_r|$ est le nombre de combinaisons p^r à p^r des éléments de G. Donc :

$$|\mathcal{P}_r| = \left(\begin{array}{c} sp^n \\ p^r \end{array} \right). \tag{461}$$

Par conséquent, d'après le lemme que nous venons de démontrer :

$$\left(\begin{array}{c} sp^n \\ p^r \end{array} \right) = \lambda p^{n-r}, \tag{462}$$

avec $p \nmid \lambda$.
Donc, p^{n-r+1} ne divise pas $\left(\begin{array}{c} sp^n \\ p^r \end{array} \right)$.
Ce qui contredit notre hypothèse.
Donc, il existe j tel que :

$$p^{n-r+1} \nmid \frac{|G|}{|A_j^G|}. \tag{463}$$

3) Soit $H = A_j^G$.
Montrons que H est d'ordre p^r.
Nous avons :

$$|G| = \frac{|G|}{|H|}|H|, \tag{464}$$

avec :

$$p^n \quad | \quad |G| \tag{465}$$

$$p^{n-r+1} \quad \nmid \quad \frac{|G|}{|H|}. \tag{466}$$

Donc, nécessairement, $p^r || H|$.
Soit $x \in A_j$.
H est stabilisateur de A_j, donc :

$$\forall h \in H, \quad hx \in A_j. \tag{467}$$

Donc, on peut définir une application :

$$\begin{array}{rccc} \phi : & H & \longrightarrow & A_j \\ & h & \longmapsto & hx. \end{array} \tag{468}$$

Cette application est évidemment injective, puisque si :

$$hx = h'x, \tag{469}$$

alors on obtient :

$$h = h', \tag{470}$$

par multiplication à droite par l'inverse x^{-1}.
Donc, l'injectivité impose :

$$|H| \leq |A_j|. \tag{471}$$

D'où :

$$|H| \leq p^r. \tag{472}$$

En résumé, nous avons démontré que $p^r || H|$ et $|H| \leq p^r$.
Donc $|H| = p^r$.
Donc H est un p-sous-groupe de G d'ordre p^r.
Par conséquent, pour tout $r \in [1, n]$, il existe un p-sous-groupe de G d'ordre p^r.
Donc, a fortiori, il existe un p-Sylow de G.

C.Q.F.D.

EURISTIDE : Il faut comprendre ici que nous avons démontré un résultat plus fort encore que le premier théorème de Sylow : dans un groupe d'ordre mp^n, pour chaque r tel que $1 \leq r \leq n$, il existe un p-sous-groupe de G d'ordre p^r.

BEATRIX : Et l'un d'entre eux est un p-Sylow.

MATHINE : Voyons maintenant le deuxième théorème de Sylow.

Théorème **7.2.2 (Deuxième théorème de Sylow)** *Soit G un groupe (cf. 4.1.5) de cardinal (cf. 4.4.3) n, n vérifiant $n = p^\alpha.m$ avec p premier et p ne divisant pas m. G contient, d'après le premier théorème de Sylow (cf. 7.2.1), un ou des p-Sylow (cf. 7.2.2). Les p-Sylow de G sont tous conjugués (cf. 5.4.2). De plus leur nombre k divise n.*

EURISTIDE : Le fait que les p-Sylow de G soient tous conjugués peut se comprendre à partir du lemme que nous avons démontré tout à l'heure. Dès lors qu'on a trouvé un p-Sylow, on peut le mettre en relation de conjugaison avec les autres p-Sylow.
L'action de conjugaison sur les p-Sylow est invariante sur l'ensemble des p-Sylow, puisque tous les p-Sylow sont conjugués.
Et par conséquent, on peut considérer l'ensemble des p-Sylow comme l'unique orbite de cette action. Et par conséquent, son cardinal divise l'ordre du groupe G.

MATHINE : Voyons la démonstration.

Démonstration :

Soit E l'ensemble des p-Sylow $\{S_1, \ldots, S_k\}$ de G.

1) Montrons que tous les p-Sylow sont conjugués.
   D'après le lemme que nous avons démontré précédemment, pour tout i tel que $1 \leq i \leq k$, puisque S_1 est un sous-groupe de G, il existe un élément $a \in G$ tel que :
   $$aS_1a^{-1} \cap S_i, \tag{473}$$
   soit un p-Sylow de S_i.
   Or, aS_1a^{-1} a même cardinal que S_1. Donc aS_1a^{-1} et S_i ont pour cardinal p^r, et leur intersection également. Donc :
   $$aS_1a^{-1} = S_i. \tag{474}$$
   Donc, tous les p-Sylow sont conjugués.
2) Montrons que le nombre de p-Sylow divise $|G|$.
   Considérons l'action de G sur E :
   $$g.S_i = gS_ig^{-1}. \tag{475}$$

Comme tous les p-Sylow sont conjugués, cette action est correctement définie.
Par ailleurs, puisque tous les p-Sylow sont conjugués, il en résulte également que cette action ne possède qu'une seule orbite. Et par conséquent, le cardinal de cette unique orbite est $|E|$. Or nous savons que le cardinal d'une orbite divise l'ordre du groupe G, donc :

$$|E||G|. \tag{476}$$

C.Q.F.D.

BEATRIX : Dans les quelques démonstrations que nous avons vues récemment, le détour par la théorie des actions sur un groupe pour démontrer des propriétés sur les cardinaux s'est toujours avéré très efficace !

EURISTIDE : Nous allons maintenant aborder le troisième et dernier théorème de Sylow. Il nous donne une règle sur le nombre de p-Sylow dans un groupe G.

MATHINE : Le voici.

Théorème 7.2.3 (Troisième théorème de Sylow) *Soit G un groupe (cf. 4.1.5) de cardinal (cf. 4.4.3) n, n vérifiant $n = p^{\alpha}.m$ avec p premier et p ne divisant pas m. G contient, d'après le premier théorème de Sylow (cf. 7.2.1), un ou des p-Sylow (cf. 7.2.2). Le nombre k de p-Sylow dans G vérifie $k \equiv 1 (mod. p)$.*

EURISTIDE : Si l'on considère l'ensemble E des p-Sylow et l'action de conjugaison de G sur E, on voit que pour un p-Sylow donné S, le seul élément de E^S (ensemble des éléments de E dont l'orbite est réduite à un seul élément, donc conjugués d'eux-mêmes) est S lui-même.
Or, nous savons que :

$$|E| \equiv |E^S| \pmod{p}, \tag{477}$$

puisque S est un p-Sylow, donc un p-groupe.
Donc :

$$|E| \equiv 1 \pmod{p}. \tag{478}$$

MATHINE : Voyons maintenant la démonstration formelle.

Démonstration :

1) Considérons l'ensemble E des p-Sylow de G.
Considérons l'action de conjugaison de G sur E, c'est-à-dire si $g \in G$ et $S \in E$:

$$g.S = gSg^{-1}. \tag{479}$$

On considère l'action de S sur E, restriction à S de l'action de G.

2) Soit E^S le fixateur de E sous l'action de S. Ce sont donc les éléments de E dont l'orbite est constituée d'un unique point.
Donc $S' \in E^S$ est équivalent à :
$$\forall g \in G, \quad g.S'.g^{-1} \subseteq S. \tag{480}$$
Considérons le sous-groupe H engendré par S' et S. Alors la relation :
$$\forall g \in G, \quad g.S'.g^{-1} \subseteq S \tag{481}$$
implique que S' est distingué dans H. Donc S' est égal à tout autre sous-groupe qui lui est conjugué. En particulier, puisque S et S' sont des p-Sylow de H, et que par conséquent, ils sont conjugués, alors :
$$S' = S. \tag{482}$$
Donc, l'unique élément de E^S est S.

3) Par conséquent :
$$|E^S| = 1. \tag{483}$$
Or, puisque S est un p-groupe, nous avons :
$$|E| \equiv |E^S| \pmod{p}. \tag{484}$$
Donc, finalement :
$$|E| \equiv 1 \pmod{p}. \tag{485}$$

C.Q.F.D.

EURISTIDE : Nous allons finir par un corollaire qui se déduit immédiatement de ce que nous avons vu jusqu'ici.

MATHINE : En effet, nous allons pouvoir déduire des propriétés supplémentaires sur le nombre de p-Sylow.

Corollaire 7.2.1
Nombre de p-Sylow
Soit G un groupe (cf. 4.1.5) de cardinal (cf. 4.4.3) n, n vérifiant $n = p^\alpha.m$ avec p premier et p ne divisant pas m. Soit k le nombre de p-Sylow (cf. 7.2.2) dans G. Alors k divise m et k est premier avec p.

Démonstration :

Nous savons que le nombre k de p-Sylow de G est congru à 1 modulo p :
$$k \equiv 1 \pmod{p}. \tag{486}$$
Par conséquent, k ne divise par p, et donc ces deux entiers sont premiers entre eux :
$$(k, p) = 1. \tag{487}$$

Mais, d'après le deuxième théorème de Sylow, k divise n. Donc k divise $m.p^\alpha$ et est premier avec p, donc k divise m.

C.Q.F.D.

EURISTIDE : Voilà. Nous avons terminé de présenter les théorème de Sylow.

BEATRIX : Les démonstrations en étaient intéressantes. Nous y avons fait appel à des notions de divisibilité, et groupes quotients, d'action d'un groupe sur un ensemble, sans parler des sous-groupes distingués. Bref, un beau parcours dans les différentes notions que nous avons abordées jusqu'ici.

EURISTIDE : Les p-Sylow et les p-groupes établissent un pont entre le domaine des groupes (dont plus généralement de l'Algèbre) et le domaine de la théorie des nombres. C'est pourquoi ces p-Sylow nous seront de nouveau très utiles lorsque nous aborderons la démonstration du théorème de Fermat-Wiles.
Avant de quitter le domaine des groupes, nous allons établir en vrac quelques définitions complémentaires qui nous seront nécessaires par la suite.

8 Acte VII - Autres définitions

MATHINE : Commençons par définir un co-ensemble.

Définition **8.0.3**
Co-ensemble
Soit G un groupe (cf. 4.1.5). Soit H un sous-groupe (cf. 4.2.1) de G. Soit $x \in G$. Soit $xH = \{xh; h \in H\}$ et $Hx = \{hx; h \in H\}$. Un sous-ensemble de G de la forme xH pour un certain $x \in G$ est appelé co-ensemble gauche de H. Un sous-ensemble de G de la forme Hx pour un certain $x \in G$ est appelé co-ensemble droit de H.

EURISTIDE : Les co-ensembles sont en quelque sorte le reflet dans le miroir des classes à gauche et à droite d'un élément de x modulo le sous-groupe H.

BEATRIX : Oui, c'est vrai, je me le rappelle : xH était la classe à droite de x modulo H, et Hx était la classe à gauche de x modulo H.

EURISTIDE : Alors, changeons de point de vue maintenant. Au lieu de prendre le point de vue de l'élément x, prenons celui du sous-groupe H. xH est le co-ensemble à gauche de H, et Hx est le co-ensemble à droite.

BEATRIX : Question de point de vue effectivement ! Et l'image du reflet dans le miroir est tout à fait judicieuse, puisque droite et gauche sont inversés dans ce changement de point de vue : le co-ensemble de

gauche de H correspond à la classe à droite de x et le co-ensemble de droite de H correspond à la classe à gauche de x !

MATHINE : Voyons maintenant la notion de classe de groupe.

Définition **8.0.4**
Classe de groupe
On appelle classe de groupe l'ensemble complet des éléments d'un groupe mutuellement conjugués.

EURISTIDE : On considère en effet tous les éléments qui sont conjugués deux à deux, c'est-à-dire les éléments x et y deux à deux tels qu'il existe $g \in G$ tel que :

$$x = gyg^{-1}. \tag{488}$$

BEATRIX : Cette notion a bien un sens parce qu'elle est transitive : si x et y sont mutuellement conjugués, et si y et z le sont également, alors :

$$x = gyg^{-1} \tag{489}$$
$$y = g'zg^{'-1}. \tag{490}$$

Donc :

$$x = gg'zg^{'-1}g^{-1} \tag{491}$$
$$= (gg')z(gg')^{-1}. \tag{492}$$

Et par conséquent x et z sont bien mutuellement conjugués.

EURISTIDE : Donc, pour constituer la classe de groupe, il faut y placer, après le premier couple d'éléments conjugués mutuellement, des éléments conjugués avec au moins un élément de la classe de groupe.

MATHINE : Voyons enfin la notion de torsion d'un groupe.

Définition **8.0.5**
Groupe de torsion
Soit G un groupe (cf. 4.1.5). Les éléments de torsion $Tor(G)$ de G (également appelés la torsion de G) sont définis comme l'ensemble des éléments g dans G tels que $g^n = e$ pour un entier naturel n, où e est l'élément neutre (cf. 4.1.3) du groupe G.
Dans le cas où G est abélien (cf. 4.1.7), $Tor(G)$ est un sous-groupe (cf. 4.2.1) et est appelé sous-groupe de torsion de G.
Si $Tor(G)$ consiste uniquement en l'élément neutre e de G, le groupe G est dit sans torsion .

EURISTIDE : Un groupe sans torsion garantit qu'aucun autre élément que e ne s'annihile lui-même.
Par exemple, le groupe des entiers relatifs muni de l'addition est sans torsion.

`BEATRIX` : En revanche, le groupe $G = \{0, 1, 2, 3\}$;, muni de la loi :

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

possède une torsion. En effet :

$$0 = 1 \oplus 1 \oplus 1 \oplus 1 \quad (493)$$
$$0 = 2 \oplus 2 \quad (494)$$
$$0 = 3 \oplus 3 \oplus 3 \oplus 3. \quad (495)$$

Donc $Tor(G) = \{0, 1, 2, 3\} = G$.

`EURISTIDE` : La condition de commutativité requise pour que $Tor(G)$ soit un sous-groupe provient de ce que si $g^n = e$ et $g^{'m} = e$, alors l'expression $(gg')^{mn}$ requiert la commutativité de la loi de groupe pour pouvoir isoler $g^{mn}g^{'mn}$ et obtenir un produit assuré d'être dans $Tor(G)$.
A noter de plus que la torsion d'un groupe contient nécessairement au moins l'élément neutre. C'est pourquoi la torsion d'un groupe dit sans torsion est réduite à $\{e\}$.

`MATHINE` : Voilà. Nous avons fini notre parcours dans le monde des groupes.

`BEATRIX` : C'était un beau voyage dans l'abstraction. Si je résume rapidement, nous avons commencé par définir les relations d'équivalence qui nous ont permis d'apprendre à simplifier les ensembles en y construisant des classes d'individus et un ensemble quotient qui réunit ces classes. L'ensemble quotient est donc une sorte de simplification de l'ensemble de départ où l'on regarde les classes d'individus plutôt que les individus eux-mêmes.
Puis, nous nous sommes intéressés à la notion d'ensembles ordonnés.
Dans l'étape suivante, nous avons construit la structure de groupe et de certaines de ses parties, les sous-groupes. Nous avons alors pu définir une catégorie d'applications entre groupes, qui conservent les structures de groupes et sont compatibles avec celles-ci : les homomorphismes. Nous avons alors découvert avec émerveillement que le noyau et l'image d'un homomorphisme sont des sous-groupes.
Nous avons ensuite regardé d'un peu plus près des sortes de groupes particuliers : les groupes finis, les groupes monogènes, les groupes cycliques. Cela était l'occasion de définir la notion d'ordre d'un groupe (son cardinal) et d'ordre d'un élément.
Alors, nous avons pu attaquer une de mes parties préférées : les groupes quotients ; à l'instar de ce que nous avons fait pour les ensembles quotients, nous avons construit une simplification en considérant les classes d'éléments qui sont identiques à un multiple près pris dans un sous-groupe donné. Cette construction n'a pu avoir de sens qu'à condition que le sous-groupe choisi pour le quotient possède une certaine forme faible de commutativité : c'est-à-dire qu'il soit distingué.
Et voilà le meilleur moment : nous avons découvert avec curiosité que le noyau d'un homomorphisme était

un sous-groupe distingué. C'était l'occasion rêvée de construire un groupe quotient à partir de ce noyau, et c'était également l'opportunité de simplifier un homomorphisme non injectif en le rendant injectif à condition de transporter l'homomorphisme dans le groupe quotient. Ceci nous a permis de définir un homomorphisme bijectif (l'isomorphisme) entre le groupe quotient par le noyau et l'image de l'homomorphisme : ceci était l'objet des théorèmes d'isomorphisme.
Nous avons ensuite utilisé la structure de groupe pour agir sur des ensembles et y définir toute une faune de nouveaux objets tels qu'orbites, stabilisateurs, fixateurs.
Enfin, ces notions nous ont permis de construire un magnifique pont entre la théorie des groupes et la théorie des nombres, en considérant des groupes dont le cardinal est une puissance de nombre premier : les p-groupes et les p-Sylow. Nous avons alors démontré les trois théorèmes de Sylow qui permettent de mieux cerner les propriétés et le nombre de ces sous-groupes p-Sylow.
Et voilà.

`EURISTIDE` Merci, Béatrix, pour ce résumé. Nous allons pouvoir passer maintenant au plat suivant : la théorie des anneaux et des corps.

Index