

Théorie des groupes

E Vieillard-Baron

Août 2001

Table des matières

1	Relations d'équivalence	1
1.1	Introduction	1
1.2	Vocabulaire	1
1.3	Ensemble quotient	2
2	Ensembles ordonnés et axiome de choix	3
2.1	Introduction	3
2.2	Ensembles ordonnés	3
2.3	Ensembles inductifs et lemme de Zorn	4
3	Groupes	6
3.1	Introduction	6
3.2	Vocabulaire	7
3.3	Sous groupe d'un groupe	8
3.4	Homomorphisme de groupe	8
3.5	Notions supplémentaires sur les groupes	10
4	Groupes quotients	11
4.1	Introduction	11
4.2	Construction du quotient d'un groupe	11
4.3	Structure de l'ensemble quotient d'un groupe	14
4.4	Théorèmes d'isomorphie	15
4.5	Quelques définitions supplémentaires	17
5	Action de groupe	19
5.1	Introduction	19
5.2	Définition	19
5.3	Propriétés	20
6	Théorème de Cauchy et théorèmes de Sylow	23
6.1	Introduction	23
6.2	Théorème de Cauchy	23
6.3	Théorèmes de Sylow	24

Chapitre 1

Relations d'équivalence

Par Emmanuel Vieillard Baron

1.1 Introduction

La notion de relation d'équivalence est un outil merveilleux.

Elle permet tout d'abord de réunir des objets "équivalents" dans une même classe et ainsi de les réunir et de les traiter comme un seul. C'est le cas par exemple lorsque l'on construit le groupe fondamental d'une surface (ou d'une variété). On considère comme équivalents, des chemins tracés sur la surface considérée, et qui peuvent se ramener l'un sur l'autre par une déformation continue de l'un des deux chemins. Un autre exemple, beaucoup plus élémentaire, est donné par la relation d'équivalence suivante: " l'entier n est équivalent à l'entier m si $m-n$ est paire". On aura alors une partition de \mathbb{N} en deux sous ensembles: ceux qui seront équivalents à 1 et qui seront les nombres impairs d'une part, ceux qui seront équivalents à 2 et qui seront les nombres pairs, d'autre part.

Le second intérêt de cette notion est de permettre la création de nouveaux objets mathématiques. Les exemples sont nombreux et parmi les plus célèbres, citons les corps finis \mathbb{F}_p sur lesquels nous reviendrons dans une prochaine de leçon, l'espace projectif réel ou complexe de dimension n $kP[n]$ où k désigne \mathbb{R} ou \mathbb{C} , ou encore la bouteille de Klein obtenue en découpant un tore le long d'un de ses cercles générateurs et en le "recollant" via une "bonne relation d'équivalence".

Dans toute la leçon X désignera un ensemble quelconque non vide.

1.2 Vocabulaire

Définition On considère une relation \mathcal{R} sur un ensemble X . On dira que \mathcal{R} est une **relation d'équivalence** si pour tout x, y et z de X elle vérifie:

- \mathcal{R} est **réflexive**: $x \mathcal{R} x$.
- \mathcal{R} est **symétrique**: $x \mathcal{R} y \Leftrightarrow y \mathcal{R} x$.

1.3. ENSEMBLE QUOTIENT

– \mathcal{R} est **transitive**: si $x \mathcal{R} y$ et que $y \mathcal{R} z$ alors $x \mathcal{R} z$.

Exemple "être égal à" est une relation d'équivalence (sur n'importe quel ensemble X).

Exemple Sur \mathbb{Z} , on considère la relation $x \mathcal{R} y \Leftrightarrow x-y$ est pair où x et y désignent des éléments quelconques de \mathbb{Z} . \mathcal{R} ainsi définie est une relation d'équivalence (le vérifier!!).

Définition Soit X un ensemble muni d'une relation d'équivalence \mathcal{R} . Soit aussi x un élément de X . On appellera **classe d'équivalence de x suivant \mathcal{R}** l'ensemble $\{y \in X ; y \mathcal{R} x\}$. Un élément y d'une classe d'équivalence sera appelé **un représentant** de la classe d'équivalence.

Exemple Pour $X=\mathbb{Z}$ et avec la relation d'équivalence définie dans l'exemple précédent, la classe d'équivalence de 2 est, comme annoncé dans l'introduction, l'ensemble des nombres pairs. La classe d'équivalence de 1 est l'ensemble des nombres impairs. Remarquons de plus que ces deux classes d'équivalence partitionnent \mathbb{Z} .

Proposition Une classe d'équivalence n'est jamais vide (!!).

Proposition Si des éléments x et y de X sont dans une même classe d'équivalence alors leurs classes d'équivalences sont identiques.

Exemple Dans l'exemple précédent, la relation d'équivalence choisie nous fournit exactement deux classes d'équivalence sur \mathbb{Z} . Tout élément de \mathbb{Z} a sa classe d'équivalence égale à une de ces deux là.

Proposition fondamentale L'ensemble des classes d'équivalence d'un ensemble X pour une relation d'équivalence donnée \mathcal{R} définit une partition de X .

Démonstration D'une part, tout élément de X est élément d'une classe d'équivalence de la relation \mathcal{R} . Au pire, cet élément constitue à lui seul une classe d'équivalence. D'autre part, si deux classes d'équivalence s'intersectaient en un ensemble non vide, alors de part la transitivité de la relation d'équivalence \mathcal{R} , ceci impliquerait qu'elles seraient en fait égales. L'ensemble des classes d'équivalence d'une relation \mathcal{R} sur X définit ainsi bien une partition de X .

1.3 Ensemble quotient

Définition On appelle **ensemble quotient de l'ensemble X pour la relation d'équivalence \mathcal{R}** l'ensemble des classes d'équivalence de la relation \mathcal{R} . On note cet ensemble X/\mathcal{R} . A tout élément de X on peut associer la classe d'équivalence correspondante. Cela définit une application

$$- : X \longrightarrow X/\mathcal{R} \quad x \longrightarrow \bar{x}.$$

Chapitre 2

Ensembles ordonnés et axiome de choix

Par Emmanuel Vieillard Baron

2.1 Introduction

L'axiome de choix est un axiome rajouté à ceux de la théorie des ensembles. Les mathématiques ne sauraient exister sans cet axiome. C'est grâce à lui, que l'on peut, par exemple, affirmer l'existence du supplémentaire d'un sous espace vectoriel dans un espace vectoriel de dimension infini. Pourtant, depuis son apparition dans les mathématiques, il n'a cessé d'engendrer les polémiques et les problèmes. De lui découle des paradoxes tel que celui de Banach-Tarski. Le droit à son utilisation divise encore les mathématiciens. Ce petit chapitre a pour but d'expliquer le lemme de Zorn, qui est équivalent à l'axiome de choix. Ce lemme sera utile à de nombreuses reprises par la suite.

2.2 Ensembles ordonnés

Définition Soit E un ensemble. Un **ordre partiel** sur E est donné par une relation \mathcal{R} vérifiant, si $x, y \in E$:

- \mathcal{R} est réflexive: $x\mathcal{R}x$.
- \mathcal{R} est transitive: si $x\mathcal{R}y$ et $y\mathcal{R}z$ alors $x\mathcal{R}z$.
- \mathcal{R} vérifie: si $x\mathcal{R}y$ et $y\mathcal{R}x$ alors $x=y$.

On notera \leq les relations d'ordre partiel par analogie avec la relation "être plus grand ou égal à" qui définit un ordre partiel sur \mathbb{N} , par exemple.

Définition Soit E un ensemble muni d'un ordre partiel \mathcal{R} . On dit que les 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.

2.3. ENSEMBLES INDUCTIFS ET LEMME DE ZORN

Définition Un ensemble est dit **partiellement ordonné** si il existe une relation sur E définissant un ordre partiel sur E .

Définition Soit E un ensemble partiellement ordonné et F une partie de E . F est alors lui aussi partiellement ordonné pour l'ordre induit de celui de E . On dit que **F est partiellement ordonné pour l'ordre partiel induit de F** .

Définition Soit E un ensemble partiellement ordonné pour une 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 b de E tel que $\forall x \in E x \leq b$.

Définition Soit E un ensemble partiellement ordonné pour une relation \leq . Un élément b de E est dit **élément maximal** si il vérifie: si $\exists x \in E x \leq b$ alors $x=b$. De même on définirait un **élément minimal de E** .

Définition Soit E un ensemble muni d'une relation \leq qui fait de lui un ensemble partiellement ordonné. Si pour tout x et y de E , une et une seule des deux relations: $x \leq y$ ou $y \leq x$ est réalisée alors E est dit **totalelement ordonné**.

Définition Soit E un ensemble partiellement ordonné et 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 $\forall x \in F, x \leq b$.

Définition Soit E un ensemble partiellement ordonné et 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 de F : a est un minorant de F et si x est un minorant de F alors $x \leq a$. De même la **borne supérieure** b de F est le plus petit des majorants de F : b est un majorant de F et si x est un majorant de F alors $b \leq x$.

Remarque Attention la borne supérieure (resp. inférieure) d'un ensemble n'existe pas forcément.

2.3 Ensembles inductifs et lemme de Zorn

Définition Soit E un ensemble partiellement ordonné. E est dit **inductif** si toute partie de E non vide et totalelement ordonnée possède un majorant.

Définition Soit E un ensemble partiellement ordonné. Une partie de E totalelement ordonnée est appelée **une chaîne**. Un élément d'une chaîne est appelé **un maillon**.

Un ensemble inductif est donc aussi un ensemble dans lequel toutes chaînes possède un majorant.

Définition Un ensemble E partiellement ordonné est dit **strictement inductif** si toute partie non vide de E possède une borne supérieure.

2.3. ENSEMBLES INDUCTIFS ET LEMME DE ZORN

Lemme de Zorn Tout ensemble ordonné non vide et inductif possède un élément maximal.

Ce lemme est en fait une conséquence directe de l'axiome de choix. Nous considérerons dans ce cours le lemme de Zorn comme un axiome et écarterons pour le moment l'axiome de choix de nos préoccupations.

Chapitre 3

Groupes

Par Emmanuel Vieillard Baron

3.1 Introduction

Lorsque on observe le monde physique, on ne peut que remarquer l'importance des symétries. Ces dernières structurent l'univers à notre échelle, mais aussi, comme le prouve la physique moderne, l'univers de l'infiniment grand et celui de l'infiniment petit. Mathématiquement, les symétries d'un système physique permettent de faire baisser le nombre de paramètres inconnus décrivant ce système. (A toute symétrie d'un système physique correspond **une intégrale première** de ce système).

C'est aussi une tendance naturelle de l'être humain que de rechercher la symétrie. Si on demande, par exemple, à un enfant de dessiner un triangle, la probabilité que le triangle dessiné soit isocèle ou équilatéral est plus grande que celle qu'il soit quelconque. De même, une construction symétrique nous semblera plus esthétique qu'un édifice dissymétrique.

Il a fallu cependant attendre le 19^{ème} siècle pour disposer d'un bon support conceptuel au sujet des symétries. Même si, historiquement, la notion de groupe n'est pas née avec comme objectif celui de traiter des symétries, c'est cette notion qui permit de les modéliser complètement et de les étudier dans toute leur généralité.

La notion de groupe intervient dans la plupart des disciplines mathématiques. Ainsi la théorie des groupes sera indispensable à l'étude de l'arithmétique, de l'algèbre linéaire ou bilinéaire, de la géométrie (Euclidienne et non Euclidienne),...

Le géniteur premier de la théorie des groupes fut le très romantique E. Galois. Il introduisit cette notion afin d'étudier la possibilité de résoudre les équations polynomiales de degré ≥ 5 par radicaux (c'est à dire la possibilité de trouver des formules permettant de mettre sous forme algébrique les solutions de ces équations). Il remarqua une symétrie dans l'écriture des racines des polynômes de degré < 5 , puis construisit un groupe correspondant à ces symétries (groupe de permutation). Il montra les liens entre

3.2. VOCABULAIRE

certaines des propriétés mathématiques de ce groupe et le fait que les racines du polynôme correspondant soient exprimables par radicaux. Il montra finalement que ces propriétés mathématiques n'étaient pas vérifiées si le degré du polynôme considéré était supérieur ou égale à 5.

Dans toute la leçon G désignera un ensemble non vide.

3.2 Vocabulaire

Définition On appelle **loi interne** sur G une application de $G \times G \rightarrow G$.

Remarque Par abus de langage, plutôt que de parler de loi interne sur G , on parlera de loi sur G .

Définition fondamentale Soit \perp (prononcer antitruc) une loi sur G . On dira que la loi \perp définit une structure de **groupe** sur G si:

- \perp est **associative**, c.a.d si x, y, z sont éléments de G alors $(x \perp y) \perp z = x \perp (y \perp z)$.
- Il existe un **élément neutre** e pour \perp dans G , c.a.d il existe $e \in G$ tel que $\forall x \in G, x \perp e = e \perp x = x$.
- Tout élément x de G possède un **inverse** dans G pour \perp , c.a.d $\forall x \in G \exists y \in G; x \perp y = y \perp x = e$. On notera, par analogie avec les notations habituelles pour les nombres réels, x^{-1} l'inverse de x .

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

Proposition Soit G un groupe pour la loi \perp et soit e un élément neutre de G .

1. l'élément neutre de G est unique.
2. $e^{-1} = e$.
3. Tout élément x de G possède un unique inverse.

Démonstration

1. Supposons que G possède deux éléments neutres e et e' . Alors, par définition de l'élément neutre d'un groupe, $e \perp e' = e' \perp e = e = e'$
2. Remarquons que, par définition de e , $e \perp e = e$ et donc que e est égal à son propre inverse.
3. Soient x_1 et x_2 des inverses de x dans G pour \perp . Alors par définition de l'inverse d'un élément de G ainsi que du neutre de G , $x_1 = x_1 \perp e = x_1 \perp (x \perp x_2) = (x_1 \perp x) \perp x_2 = e \perp x_2 = x_2$.

Exemple $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, (\mathbb{R}^*, \cdot) sont des groupes.

3.3. SOUS GROUPE D'UN GROUPE

Définition On dira que le groupe (G, \perp) est **abélien** si la loi \perp est commutative, c.a.d pour tout x et y dans $G: x \perp y = y \perp x$.

3.3 Sous groupe d'un groupe

Soit (G, \perp) un groupe. Notons e le neutre de G .

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

Proposition On a équivalence entre:

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

Démonstration Si H est un sous groupe de G , il est clair que la seconde partie de la proposition est validée.

Supposons donc maintenant cette deuxième partie validée et montrons que (H, \perp) a une structure de groupe. Remarquons pour commencer que comme $x \perp y^{-1}$ est élément de H pour tout élément x et y de H , on peut affirmer que la restriction de \perp sur H définit une loi interne sur H . Remarquons ensuite que comme e est élément de H , \perp possède un élément neutre dans H . De plus, si y est élément de H alors comme e est élément de H , $e \perp y^{-1}$ est élément de H et donc y possède un inverse dans H . L'associativité de la loi \perp restreinte à H provient de l'associativité de \perp sur G . (H, \perp) a donc bien une structure de groupe.

Remarque Ce critère sera très pratique pour vérifier que des ensembles munis d'une loi interne sont bien des groupes. En effet, on cherchera à montrer qu'ils sont des sous groupes d'un groupe plus grand. Il n'y aura alors que deux propriétés à vérifier à la place de 4.

Exemple $(\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{Q}, +)$.

Exemple $(\{2 \times k; k \in \mathbb{Z}\}, +)$ est un sous groupe de $(\mathbb{Z}, +)$.

3.4 Homomorphisme de groupe

On considère dans ce paragraphe deux groupes (G, \perp) et (H, \top) . On note e_G et e_H les neutres respectifs de G et H . (\top se prononce truc).

Définition 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 , $f(x \perp y) = f(x) \top f(y)$.

3.4. HOMOMORPHISME DE GROUPE

De plus:

- Si $G=H$, nous dirons que f est un **endomorphisme**.
- Si f est bijective, nous dirons que f est un **isomorphisme**. Si il existe un isomorphisme entre G et H , nous dirons que G et H sont **isomorphes** et nous noterons $G \simeq H$.
- Si f est à la fois un isomorphisme et un endomorphisme, nous dirons que f est un **automorphisme**.

Remarque La notion d'isomorphisme joue en algèbre un rôle dual à celui des homéomorphismes en topologie ou des difféomorphismes en géométrie différentielle. Des groupes qui seront isomorphes auront les mêmes propriétés algébriques. Ainsi, l'étude algébrique d'un groupe pourra se faire sur n'importe quel groupe qui lui est isomorphe.

Proposition Soit x un élément de G , $f(x^{-1}) = (f(x))^{-1}$.

Démonstration Choisissons x dans G . On a $e_H = f(e_G) = f(x \perp x^{-1}) = f(x) \top f(x^{-1})$ et donc par définition de l'inverse d'un élément d'un groupe, $f(x^{-1}) = (f(x))^{-1}$.

Définition Soit f un homomorphisme de G dans H . Nous noterons $\text{Ker } f$ ou $\text{Ker}(f)$ l'ensemble $\{x \in G; f(x) = e_H\}$. Cet ensemble s'appelle le **noyau** de l'homomorphisme f .

Remarque En allemand, noyau se dit **Kernel**.

Remarque Le noyau d'un homomorphisme n'est jamais vide. En effet, le neutre du groupe de départ est toujours élément du noyau.

Théorème Soit f un homomorphisme entre G et H . On a équivalence entre:

- f est injective.
- $\text{Ker } f$ est réduit à l'élément neutre de G .

Démonstration Si f est injective, l'image du neutre de G par f étant le neutre de H , aucun autre élément de G ne peut avoir e_H comme image. (Ou sinon cela contredit l'injectivité de f). Donc le noyau de f se réduit à $\{e_G\}$.

Si cette dernière propriété est vérifiée, prenons x et y dans G telles que $f(x) = f(y)$. Alors f étant un homomorphisme, $f(x \perp y^{-1}) = e_H$. Donc $x \perp y^{-1}$ est élément de $\text{Ker } f$. Mais le noyau de f étant réduit à $\{e_G\}$, cela implique que $x \perp y^{-1} = e_G$ et donc que $x = y$.

Proposition Soit $f : G \longrightarrow H$ un homomorphisme . Alors:

- $\text{Ker } f$ est un sous groupe de G .
- $\text{Im } f (= \text{l'image de } f = \{f(x); x \in G\})$ est un sous groupe de H .

Démonstration Montrons que le noyau de f est un sous groupe de G . e_G est naturellement élément de $\text{Ker } f$. Soient x et y des éléments de $\text{Ker } f$. Alors $f(x \perp y^{-1}) = f(x) \top f(y)^{-1} = e_H$. Ceci prouve que $x \perp y^{-1}$ est élément de $\text{Ker } f$.

Montrons maintenant que $\text{Im } f$ est un sous groupe de H . Remarquons que $e_H = f(e_G)$

3.5. NOTIONS SUPPLÉMENTAIRES SUR LES GROUPEs

et donc que e_H est élément de $\text{Im } f$. Soient encore $f(x)$ et $f(y)$ des éléments de $\text{Im } f$. Alors $f(x) \cdot f(y)^{-1} = f(x \cdot y^{-1})$ est bien élément de $\text{Im } f$. C.q.f.d.

Proposition L'application composée de deux homomorphismes est encore un homomorphisme.

Démonstration Triviale!!!

3.5 Notions supplémentaires sur les groupes

Définition Soit (G, \perp) un groupe. Soit I un sous ensemble de G . On dit que I **engendre** G si tout élément de G peut s'écrire comme un produit (via la loi \perp) d'éléments de I .

Définition Soit (G, \perp) un groupe.

- On dit que G est **finiment engendré** si il existe une partie I de G de cardinal fini et qui engendre G .
- On dira que G est **fini** si son cardinal est fini. Dans ce cas, on notera $|G|$ le cardinal de G . Le cardinal d'un groupe s'appelle aussi **l'ordre** de ce groupe.
- On dit que G est **monogène** si il est engendré par un sous ensemble constitué d'un unique élément.
- On dit que G est **cyclique** si il est monogène et fini.

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

$$g^n = \underbrace{g \perp \dots \perp g}_{n \text{ fois}}.$$

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

Proposition Si (G, \cdot) est un groupe fini alors tout élément de G a un ordre plus petit que le cardinal de G .

Démonstration Notons n le cardinal de G . Soit g un élément de G . Si l'ordre de g n'est pas fini ou plus grand que n , alors on peut trouver un entier m plus grand que n tel que $A = \{g, g^2, \dots, g^m\}$ soit un sous ensemble de G ne contenant pas l'élément neutre. Mais le cardinal de A est nécessairement plus petit que celui de G . Ceci implique l'existence de deux entiers i et j plus petit ou égaux à m et plus grand que 0 tel que $g^i = g^j$. On peut supposer $i < j$. Alors $g^{j-i} = e$. On a alors trouvé un entier $k=j-i$ tel que $0 < k < m$ et tel que $g^k = e$. Ceci contredit notre hypothèse de départ et nous permet d'affirmer que l'ordre de g est fini et plus petit que le cardinal de G .

On renvoie ici à la section sur le théorème de Lagrange pour plus de précision sur le rapport entre l'ordre d'un groupe et l'ordre d'un élément de ce groupe.

Chapitre 4

Groupes quotients

Par Emmanuel Vieillard Baron

4.1 Introduction

La notion de relation d'équivalence utilisée va nous fournir un moyen de construire des groupes. Ces groupes s'appellent les **groupes quotients** et leur importance est capitale en mathématique.

4.2 Construction du quotient d'un groupe

Dans toute cette leçon, (G, \cdot) désigne un groupe et (H, \cdot) désigne un sous groupe de G . On considère aussi la relation, si x et y sont éléments de G :

$$x\mathcal{R}y \Leftrightarrow x^{-1} \cdot y \in H.$$

Proposition La relation \mathcal{R} définie par $x\mathcal{R}y \Leftrightarrow x^{-1} \cdot y \in H$ est une relation d'équivalence.

Démonstration Triviale!!

Définition On notera G/H l'ensemble G/\mathcal{R} des classes d'équivalences de la relation \mathcal{R} sur G .

Proposition Soit $x \in G$. La classe d'équivalence de x pour la relation

$$x\mathcal{R}y \Leftrightarrow x^{-1} \cdot y \in H$$

est l'ensemble $xH = \{x \cdot h; h \in H\}$.

Démonstration Soit $y \in G$ équivalent à x pour la relation \mathcal{R} . Alors il existe $h \in H$ tel que $x^{-1} \cdot y = h$. Et donc y est élément de Hx . Réciproquement, si y est élément

4.2. CONSTRUCTION DU QUOTIENT D'UN GROUPE

de Hx , il est clair que $y \mathcal{R} x$.

Définition L'ensemble xH s'appelle **classe à gauche** de l'élément x de G .

Remarque On aurait aussi pu définir notre relation d'équivalence \mathcal{R} par:

$$x\mathcal{R}y \Leftrightarrow y.x^{-1} \in H.$$

Dans ce cas, la classe d'équivalence d'un élément x de G aurait été donné par l'ensemble Hx .

Définition L'ensemble Hx s'appelle **classe à droite** de l'élément x de G .

Proposition Si H est un sous groupe fini de G et si x et y sont deux éléments de G alors les classes d'équivalences (à gauche ou à droite) de x et y pour la relation \mathcal{R} ont même nombre d'éléments et ce nombre est égal au cardinal de H .

Démonstration Soit x un élément de G . Posons $f : H \longrightarrow xH$ $h \longrightarrow f(h) = x.h$. f est injective car si h et h' sont des éléments de H tels que $f(h) = f(h')$ alors on a l'égalité $x.h = x.h'$ et x étant élément du groupe G , ceci implique, en multipliant à gauche chacun des membres de l'égalité précédente par x^{-1} que $h=h'$. f est aussi surjective car si y est un élément de xH , alors il existe $h \in H$ tel que $y = x.h$ et donc $y = f(h)$. f étant à la fois injective et surjective, elle est bijective. Ceci prouve que H et xH ont même nombre d'éléments. Mais si y est un élément de G , yH et H auront aussi même nombre d'éléments. Donc xH et yH ont même cardinal.

De même on montrerait que toutes les classes à droite pour une relation \mathcal{R} , issue d'un sous groupe H de cardinal fini dans G , ont même nombre d'éléments, ce nombre étant égal à $|H|$.

Le théorème qui vient maintenant et qui résulte des propositions précédentes est fondamental en algèbre.

Théorème de Lagrange Soit G un groupe fini. Si H est un sous groupe de G , alors le cardinal de H divise celui de G . On notera $|G/H|$ où $[G:H]$ le nombre $|G|/|H|$. $[G:H]$ s'appelle **l'indice de H dans G** .

Démonstration Soit donc H un sous groupe de G . On considère la relation d'équivalence \mathcal{R} associée à H . Elle nous permet de définir une partition de G par des sous ensembles de la forme xH où $x \in G$. On peut donc trouver, G étant fini, un nombre $n \in \mathbb{N}$ et $x_1, \dots, x_n \in G$ tels que $\{x_1H, \dots, x_nH\}$ forme une partition de G . Mais les sous ensembles x_iH ont tous, d'après la proposition précédente, le même nombre d'éléments. De plus, ce nombre est égale à $|H|$. Donc le cardinal de G s'écrit $|G|=n|H|$. Ceci prouve notre théorème.

On donne maintenant un corollaire du théorème de Lagrange qui est absolument fondamental dans la théorie des groupes finis.

4.2. CONSTRUCTION DU QUOTIENT D'UN GROUPE

Théorème Soit G un groupe. Soit g un élément de G d'ordre fini. Alors l'ordre de g divise l'ordre de G .

Démonstration Soient G et g comme dans l'énoncé du théorème et soit n l'ordre de g . Alors $\{g, g^2, \dots, g^n = e\}$ est un sous groupe de G . Cette affirmation est triviale à vérifier. De plus, par définition de l'ordre d'un élément dans un groupe, ce sous groupe est de cardinal n . Par application du théorème de Lagrange, n est un diviseur du cardinal de G .

On se posera, un peu plus tard dans le cours, le problème réciproque, à savoir: Si p est un diviseur de l'ordre du groupe alors existe-t-il un élément d'ordre p dans G ou encore: existe-t-il un sous groupe d'ordre p dans G . La réponse sera donnée par le théorème de Cauchy pour les éléments d'ordre p et sous certaines conditions sur p , et par le théorème de Sylows, pour les sous groupes d'ordre p , sous certaines conditions sur p et sur G .

Il est naturel de se demander pour quelles conditions sur H on a coïncidence entre les classes à gauche et les classes à droite. Nous allons nous pencher sur cette question dans la fin de ce paragraphe.

Définition On dira 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 $H \triangleleft G$ le fait que H soit normal dans G .

Proposition Soit H un sous groupe du groupe fini G . Les classes à gauche et à droite de la relation d'équivalence héritée de H coïncident si et seulement si H est normal dans G .

Démonstration Supposons que les classes à gauche et à droite coïncident. Pour tout g dans G , on a: $gH = Hg$. donc en particulier, pour tout h dans H , il existe h' dans H tel que $g.h = h'.g$. Donc pour tout h dans H , il existe h' tel que $g.h.g^{-1} = h' \in H$. Ceci prouve que $H \triangleleft G$.

Réciproquement, supposons que $H \triangleleft G$. Alors pour tout g dans G et tout h dans H , $g.h.g^{-1}$ est élément de H . Donc pour tout g dans G et tout h dans H , $g.h$ est dans $H.g$. On a ainsi montré que pour tout élément g de G , $gH \subset Hg$. Comme les cardinaux de gH et Hg sont égaux à celui de H , ils sont égaux entre eux et on a alors bien $gH = Hg$.

La proposition suivante semble être anecdotique alors qu'elle est en fait fondamentale et permet de construire des groupes parmi les plus importants en Mathématique.

Proposition Si G et G' sont deux groupes et que $f : G \longrightarrow G'$ est un homomorphisme de groupe alors le noyau de f : $\text{Ker } f$ est un sous groupe normal de G .

Démonstration Je ne vous en ferais pas l'affront.

4.3 Structure de l'ensemble quotient d'un groupe

Remarque Si x est élément de G , nous noterons \bar{x} la classe d'équivalence de x dans G/H . x sera alors un représentant de la classe d'équivalence \bar{x} .

Définition Nous allons définir une loi interne \perp sur G/H par: Si x et y sont éléments de G alors

$$\bar{x} \perp \bar{y} = \overline{x.y}$$

Quand aucune confusion n'est à craindre, nous noterons la loi interne de G/H de la même façon que celle de G . Cette loi est celle **induite de G sur G/H** .

Remarque Il faut vérifier que cette loi est bien définie sur G/H , c.a.d que si x, x', y, y' sont des éléments de G tels que

$$\bar{x} = \bar{x}' \text{ et } \bar{y} = \bar{y}' \text{ alors } \overline{x.y} = \overline{x'.y'}.$$

Proposition La loi définie précédemment est bien définie si et seulement si H est normal dans G .

Démonstration La condition à vérifier pour que la loi précédente soit bien définie sur G/H est que si x, x', y, y' sont des éléments de G tels que

$$\bar{x} = \bar{x}' \text{ et } \bar{y} = \bar{y}' \text{ alors } \overline{x.y} = \overline{x'.y'}.$$

Etudions quelle propriété sur H nous permet de valider cette condition. La condition précédente est équivalente à la suivante:

$$x.x'^{-1} \in H, y.y'^{-1} \in H \Rightarrow x.y.y'^{-1}.x'^{-1} \in H.$$

Mais comme, par hypothèse, $y.y'^{-1}$ est élément de H et que tout élément de H peut s'écrire sous la forme $y.y'^{-1}$ où y est élément de G (si h est dans H on écrit $h=y.y'^{-1}$!!!), cette condition implique la suivante (qui semble bien moins restrictive):

$$x \in G \Rightarrow xHx^{-1} \in H.$$

ou, autrement dit, notre condition de départ entraîne celle que H est normal dans G . Résumons nous: La loi définie précédemment sur G/H nous assure d'une structure de groupe sur cet ensemble seulement si H est normal dans G . Montrons que cette condition est aussi suffisante: Supposons alors que H est normal dans G . Si $x.x'^{-1} \in H, y.y'^{-1} \in H$, montrons alors que $x.y.y'^{-1}.x'^{-1} \in H$. Notons $h = y.y'^{-1}$. h est élément de H . Il faut donc montrer que $x.h.x'^{-1}$ est élément de H . Mais on peut écrire: $x.h.x'^{-1} = x.h.x^{-1}.x.x'^{-1}$ et comme H est normal dans G et que $x.x'^{-1} \in H$ alors $x.h.x'^{-1}$ est bien élément de H comme produit d'éléments de H .

Théorème fondamental Supposons que H est un sous groupe normal de G . L'ensemble G/H muni de la loi interne induite de celle de G a une structure de groupe. De plus, si G est abélien il en est de même de G/H équipé de la loi induite.

Démonstration Comme H est normal dans G la loi induite par celle de G sur G/H est bien définie.

L'élément \bar{e}_G est le neutre de la loi. Dans G/H :

$$\bar{e}_G.\bar{x} = \bar{x}.\bar{e}_G = \overline{x.e_G} = \bar{x}.$$

4.4. THÉORÈMES D'ISOMORPHIE

De plus tout élément de G/H \bar{x} possède un inverse qui est $\overline{x^{-1}}$. (Donc $\overline{x^{-1}} = \bar{x}^{-1}$).

L'associativité de la loi induite se démontre en passant au quotient celle de la loi de départ. De même, on démontrerait que la loi induite est commutative si la loi de départ l'est aussi, et donc que G/H est abélien si G l'est.

4.4 Théorèmes d'isomorphie

Proposition Supposons que $H \triangleleft G$. Notons $\Pi : G \longrightarrow G/H$ l'application qui à $x \in G$ associe sa classe d'équivalence \bar{x} dans G/H . Alors Π est un homomorphisme de groupe. De plus $H = \text{Ker } \Pi$ et Π est surjectif.

Démonstration Soient x et y des éléments de G alors

$$\Pi(x.y) = \overline{x.y} = \bar{x}.\bar{y} = \Pi(x).\Pi(y).$$

Cette propriété n'est que l'expression de la définition de la loi de groupe sur G/H . Pour l'égalité entre le noyau de Π et H , il suffit de remarquer que tout élément de H est équivalent dans G/H au neutre de G/H . De plus si \bar{x} est un élément de G/H , x est un antécédent de cet élément par Π . Donc Π est bien surjectif.

Théorème Premier théorème d'isomorphisme Soient G et G' des groupes. Soit $f : G \longrightarrow G'$ un homomorphisme de groupe. Rappelons que $\text{Ker } f$ est un sous groupe distingué de G et donc que $G/\text{Ker } f$ a une structure de groupe pour la loi induite de celle de G . Rappelons aussi que l'on a un morphisme surjectif $\Pi : G \longrightarrow G/\text{Ker } f$ qui à tout élément de G associe sa classe d'équivalence dans $G/\text{Ker } f$. Ajoutons encore que l'image d'un groupe par un morphisme est un sous groupe du groupe image. On peut alors affirmer qu'il existe un isomorphisme $\bar{f} : G/\text{Ker } f \longrightarrow \text{Im } f$ tel que $\bar{f} \circ \Pi = \Pi \circ f$.

Démonstration Posons $H = \text{Ker } f$.

Construisons tout d'abord \bar{f} . Posons, si $\bar{x} \in G/H$, $\bar{f}(\bar{x}) = f(x)$ où x est un représentant de la classe d'équivalence \bar{x} . \bar{f} est bien définie car si y est un autre représentant de la classe d'équivalence associée à x , alors $\bar{f}(\bar{y}) = f(y) = f(x.x^{-1}.y) = f(x).f(x^{-1}.y)$. Cette dernière égalité est vraie car f est un morphisme et x et y étant équivalents dans G/H , $x.y^{-1}$ est élément de $\text{Ker } f$. Donc $f(y) = f(x)$ et \bar{f} est bien définie.

\bar{f} est bien, par définition, un homomorphisme de groupe.

Montrons que \bar{f} est injective. Soient $\bar{x}, \bar{y} \in G/H$. Supposons que $\bar{f}(\bar{x}) = \bar{f}(\bar{y})$ alors par définition de \bar{f} , on a: $f(x) = f(y)$ donc $f(x).f(y)^{-1} = e_{G'}$ et comme f est un homomorphisme, $f(x.y^{-1}) = e_{G'}$. Ce qui implique que $x.y^{-1} \in \text{Ker } f$ et donc que $\bar{x} = \bar{y}$. Ceci prouve l'injectivité de \bar{f} .

Comme une application est surjective sur son image (!!!) \bar{f} est un isomorphisme de G/H dans $\text{Im } f$.

Enfin par définition de \bar{f} on a bien $\bar{f} \circ \Pi = \Pi \circ f$.

Théorème Second théorème d'isomorphisme Soient G un groupe, H et K des sous groupes de G . On suppose que $H \triangleleft G$. Alors $H \cap K$ est normal dans K et $K/(K \cap H)$

4.4. THÉORÈMES D'ISOMORPHIE

$\simeq HK/H$.

Démonstration

- Montrons que $H \cap K$ est normal dans K . Il est tout d'abord évident que $H \cap K$ est un sous groupe de G (Une intersection de sous-groupes est encore un sous-groupe). Soit x un élément de $H \cap K$ et soit $g \in K$. Alors $g.x.g^{-1}$ est, comme H est normal dans G , encore élément de H . $g.x.g^{-1}$ est aussi élément de K comme produit d'élément de K . Donc $g.x.g^{-1}$ est bien élément de $H \cap K$ et $H \cap K$ est bien distingué dans K .
- Remarquons maintenant que HK est un sous groupe de G pour la loi induite de celle de G . L'élément neutre de G est naturellement élément de HK . Et si $g=h.k$, $g'=h'.k'$ sont des éléments de HK alors

$$g.g' = h.k.h'.k' = h.k.h'.k^{-1}.k.k'.$$

Comme H est normal dans G , $k.h'.k^{-1}$ est élément de H et donc égal à un élément h'' de H . Donc $g.g'=h.h''.k.k'$ est bien de la forme d'un produit d'un élément de H et d'un élément de K . Notre loi est donc bien interne. Enfin, si $g=h.k$ alors $g^{-1}=k^{-1}.h^{-1}=k^{-1}.h^{-1}.k.k^{-1}$. Comme H est normal dans G , $k^{-1}.h^{-1}.k$ est élément de H et l'inverse de g est bien élément de HK .

- $H \cap K$ étant normal dans K , $K/(K \cap H)$ a une structure de groupe pour la loi induite de celle de K . Montrons que ce groupe est isomorphe à HK/H . Définissons pour cela l'application $\theta : HK \rightarrow H/K \cap H$ par si $g=h.k$ est élément de HK , $\theta(g) = \bar{k}$ où \bar{k} désigne la classe d'équivalence de k dans $H/K \cap H$. Cette application est bien définie car si g est aussi représenté par le produit $h'.k'$ de HK alors $h.k=h'.k'$ et $k.k'^{-1}=h^{-1}.h'$. Le produit du second membre de l'égalité est élément de H et le produit du premier membre élément de K . On en déduit que $k.k'^{-1}$ est élément de $H \cap K$. Donc $\overline{k.k'^{-1}} = e_{H/H \cap K}$ et $\theta(g) = \bar{k} = \overline{k'}$. Comme $K \cap H$ est un sous groupe normal de K alors l'application θ (qui à un élément de HK associe sa classe d'équivalence...) est un homomorphisme de groupe.
- Calculons alors $\text{Ker}(\theta)$. Soit $g=h.k \in HK$ tel que $\theta(g) = \bar{k} = \overline{e_{H/H \cap K}}$. k est donc élément de $H \cap K$. Par conséquent g est un produit de deux éléments de K et est élément de K . On vient d'établir $\text{Ker}\theta \subset K$. Prenons un élément k de K . Par définition de θ , $\theta(k)=e_{H/H \cap K}$. Ceci prouve l'inclusion réciproque. En conclusion: $\text{Ker}\theta=K$.
- θ est surjective. En effet, si \bar{h} est élément de $H/H \cap K$ alors $\theta(h)=\bar{h}$.
- Appliquons enfin le premier théorème d'isomorphisme à θ : $\frac{HK}{H} \simeq \frac{H}{H \cap K}$.

Théorème Troisième théorème d'isomorphisme Soient G un groupe, H et K des sous groupes de G . On suppose que $H \triangleleft G$ et que $K \triangleleft G$. On suppose de plus que $H \subset K$. Alors $K/H \triangleleft G/H$ et

$$\frac{G/H}{K/H} \simeq G/K.$$

4.5. QUELQUES DÉFINITIONS SUPPLÉMENTAIRES

Démonstration

Soit g un élément de G . Notons \bar{x} sa classe d'équivalence dans G/H et $\bar{\bar{x}}$ sa classe d'équivalence dans G/K .

Montrons que $K/H \triangleleft G/H$. Pour cela choisissons un élément \bar{g} dans G/H et une élément \bar{k} dans K/H . Alors $\bar{g} \cdot \bar{k} \cdot \bar{g}^{-1} = \overline{g \cdot k \cdot g^{-1}}$. Mais K étant normal dans G , il existe $k' \in K$ tel que ce dernier élément soit égal à \bar{k}' , Cqfd.

Soit θ l'application qui à un élément \bar{k} de G/H associe l'élément $\bar{\bar{g}}$ de G/K . θ est bien définie et est un morphisme du groupe G/H dans le groupe G/K . De plus, H étant inclu dans K , θ est surjective. On peut alors appliquer le premier théorème d'isomorphisme. Ceci nous permet d'affirmer que

$$\frac{G/H}{K/H} \simeq G/K.$$

4.5 Quelques définitions supplémentaires

Définition On appelle **centre du groupe** (G, \perp) le sous ensemble de G $\{x \in G; \forall y \in G x \perp y = y \perp x\}$. On note $Z(G)$ ce sous ensemble. $Z(G)$ est l'ensemble des éléments de G qui commutent avec tout les autres éléments de G .

Remarque Le centre d'un groupe contient toujours l'élément neutre de ce groupe et donc est toujours non vide.

Proposition Le centre d'un groupe est un sous groupe distingué de ce groupe.

Démonstration C'est très facile.

Définition On dit que deux sous groupes H et K de G sont **conjugués** si il existe un élément g de G tel que $g.H.g^{-1}=K$.

Proposition Si deux sous groupes de G sont conjugués alors ils sont en bijection. Dans le cas où leur cardinal est fini, ils ont même cardinal.

Démonstration Soient H et K deux sous groupes conjugués de G . Soit donc g dans G tel que $g.H.g^{-1}=K$. Définissons $\theta : H \rightarrow K$ $\theta(h) = g.h.g^{-1}$. L'égalité $g.H.g^{-1}=K$ nous permet d'être convaincu de la surjectivité de θ . Pour l'injectivité: si $g.h.g^{-1} = g.h'.g^{-1}$ alors en multipliant cette égalité à gauche par g^{-1} et à droite par g , on obtient $h=h'$, Cqfd.

Définition On dit qu'un groupe est **simple** si les seuls sous groupes distingués de G sont G et $\{e\}$.

Définition On appelle **commutateur des éléments g et g'** de G l'élément de G noté $[g, g']$ et donné par $[g, g'] = g.g'.g^{-1}.g'^{-1}$.

4.5. QUELQUES DÉFINITIONS SUPPLÉMENTAIRES

Définition (Proposition) L'ensemble des commutateurs des éléments de G engendre un sous groupe distingué de G appelé **sous groupe dérivé** de G et est noté $D(G)$.

Démonstration Facile, il suffit d'écrire.

L'intérêt du sous groupe dérivé d'un groupe réside dans le fait que $G/D(G)$ est le plus grand quotient abélien de G . Ceci signifie que si H est un sous groupe normal de G tel que G/H est abélien, alors on a une injection de G/H dans $G/D(G)$.

Proposition $G/D(G)$ est le plus grand quotient abélien de G .

Démonstration Montrons tout d'abord que $G/D(G)$ est abélien (On ne rappellera pas que $G/D(G)$ a, comme $D(G)$ est normal dans G , une structure de groupe). Soient \bar{g} et \bar{g}' des éléments de $G/D(G)$. Alors comme $[g, g']$ est élément de $D(G)$, on a $\bar{e} = \overline{[g, g']} = \overline{g \cdot g' \cdot g^{-1} \cdot g'^{-1}} = \overline{g \cdot g' \cdot g^{-1} \cdot g'^{-1}}$. Donc $\bar{g} \cdot \bar{g}' = \overline{g \cdot g'}$. Comme g et g' sont quelconques dans G , on a bien montré que $G/D(G)$ est abélien. Remarquons maintenant que si H est un sous groupe normal de G tel que G/H est abélien, alors si g et g' sont éléments de H et si \bar{g} désigne la classe d'équivalence de g dans G/H , $\overline{\bar{g} \cdot \bar{g}'} = \overline{g \cdot g'}$. Soit encore $\overline{g \cdot g' \cdot g^{-1} \cdot g'^{-1}} = \bar{e}$. Cette dernière égalité prouve que $[g, g']$ est élément de H . Comme g et g' sont quelconques dans G , nous venons d'établir que $D(G) \subset H$. Montrons l'existence d'une injection de G/H dans $G/D(G)$. Soit $\theta : G/H \rightarrow G/D(G)$ telle que si g est élément de G , $\theta(\bar{g}) = \bar{g}$. On vérifie que θ est bien définie et que c'est un homomorphisme de groupe. Si $\theta(\bar{g}) = \bar{e}$ alors cela signifie que $g \in D(G)$. Mais d'après l'inclusion précédente, cela signifie aussi que $g \in H$ et donc que $\bar{g} = \bar{e}$, Cqfd.

Chapitre 5

Action de groupe

Par Emmanuel Vieillard Baron

5.1 Introduction

Certains ensembles mathématiques sont en interaction avec d'autres. Par exemple l'ensemble des symétries d'un cube est en interaction avec l'ensemble des sommets de ce cube: chaque symétrie du cube a pour effet de permuter les sommets du cube. L'ensemble des isométries de l'espace affine est en interaction avec l'ensemble des points de cet espace: à tout couple formé par une isométrie et un point x de l'espace, on peut associer le point image de l'isométrie au point x . La théorie des actions de groupe est née du besoin de formaliser et d'étudier ces interactions. Ces actions de groupes permettront aussi, couplées avec la notion de relation d'équivalence, de réunir des objets d'un ensemble suivant certaines caractéristiques ou qualités. Là encore nous disposerons d'un moyen de fabriquer de nouveaux ensembles mathématiques. Le champ d'intervention des actions de groupe se situe au niveau des mathématiques toutes entières.

5.2 Définition

Dans tout le paragraphe qui vient, X désignera un ensemble et (G, \cdot) un groupe. On notera e le neutre de G .

Définition On dira que le groupe G **agit** (ou **opère**) sur l'ensemble X si il existe une application $\theta : G \times X \longrightarrow X$ telle que:

- Pour tout x dans X , $\theta(e, x) = x$.
- Pour tout $g_1, g_2 \in G$, $\theta(g_1, \theta(g_2, x)) = \theta(g_1 \cdot g_2, x)$.

On dira aussi que θ définit une action de G sur X .

Remarque Afin de simplifier les notations, et quand aucune confusion n'est à craindre, on écrira, si $g \in G$ et $x \in X$ $\theta(g, x) = g \cdot x$.

5.3. PROPRIÉTÉS

Définition Soit θ une action de G sur X . On dira que l'action est **fidèle** si θ vérifie: $\forall x \in X \ g.x=x$ alors $g=e$.

Définition On dira que l'action θ de G sur X est **transitive** si $\forall x,y \in X \exists g \in G/g.x = y$.

Définition Soit $x \in X$ et soit θ une action de G sur X .

- On appelle **stabilisateur de x** et on note $\text{stab}(x)$ le sous ensemble de G donné par $\text{stab}(x)=\{g \in G/g.x = x\}$.
- On appelle **orbite de x** et on note $w(x)$ le sous ensemble de X donné par $\{g.x/g \in G\}$.

Définition Si g est élément de G et que θ est une action de G sur X , on appelle **fixateur de g** et on note $\text{fix}(g)$ ou X^g le sous ensemble de X donné par $\text{fix}(g)=\{x \in X/g.x = x\}$. De même si K est une partie de G , on notera X^K l'ensemble des $x \in X$ tels que $\forall g \in K/g.x = x$.

5.3 Propriétés

Dans tout ce paragraphe on s'intéresse à un groupe G agissant sur un ensemble X via une action θ .

Proposition La relation sur X définie par: si $x, y \in X, x \sim y \Leftrightarrow y \in w(x)$ est une relation d'équivalence sur X .

Démonstration Comme d'habitude réflexivité, symétrie, transitivité...

Remarque Les actions de groupes nous permettront donc de partitionner des ensembles suivant des classes d'équivalence.

Proposition Si x est élément de X alors $\text{Stab}(x)$ est un sous groupe de G .

Démonstration Remarquons que e est toujours élément de $\text{stab}(x)$. Remarquons aussi que si $g \in \text{stab}(x)$ alors $x=e.x=(g^{-1}.g).x=(g^{-1}.(g.x))=g^{-1}.x$. Donc g^{-1} est élément de $\text{Stab}(x)$. Soient maintenant $g, g' \in \text{stab}(x)$, alors on vérifie facilement que $g.g'^{-1} \in \text{Stab}(x)$.

Proposition Si x et $y \in X$ sont éléments d'une même orbite alors $\text{stab}(x)$ et $\text{stab}(y)$ sont des sous groupes conjugués de G .

Démonstration Comme x et y sont dans une même orbite, il existe $h \in G$ tel que $h.x=y$. Mais alors si $g \in \text{stab}(x)$, $h.g.h^{-1} \in \text{stab}(y)$: $h.g.h^{-1}.y=h.g.x=h.x=y$. Donc $h \cdot \text{Stab}(x) \cdot h^{-1} \subset \text{Stab}(y)$. On montrerait de même que $h^{-1} \cdot \text{Stab}(y) \cdot h \subset \text{Stab}(x)$, Ce qui nous prouve que $h \cdot \text{Stab}(x) \cdot h^{-1} = \text{Stab}(y)$ et que ces deux sous groupes sont conjugués.

Proposition Soit $x \in X$. On a une bijection entre $G/\text{stab}(x)$ et $w(x)$.

5.3. PROPRIÉTÉS

Démonstration Afin de le démontrer cela nous allons définir une application $f : G/\text{Stab}(x) \longrightarrow w(x)$ par : si $\bar{g} \in G/\text{Stab}(x)$ alors $f(\bar{g})=g.x$.

Montrons que f est bien définie: si g et g' sont des représentants de \bar{g} alors il existe $h \in \text{Stab}(x)$ tel que $g'=g.h$. Donc $g'.x=g.h.x=g.x$. f ne dépend donc pas du représentant de \bar{g} choisie et est donc bien définie.

Montrons que f est injective: Si $g.x=g'.y$ alors $g'^{-1}.g$ est élément de $\text{Stab}(x)$. Autrement dit $g'^{-1}.g = \bar{e}$ et $\bar{g} = \bar{g}'$. f est donc injective.

f est surjective: Si $y \in w(x)$ alors par définition de $w(x)$, il existe $g \in G$ tel que $g.x=y$. Donc $f(\bar{g})=y$.

La proposition est maintenant démontrée.

Corollaire Si G est fini, $\frac{|G|}{|\text{Stab}(x)|}=|w(x)|$. (Si A est un ensemble $|A|$ désigne le cardinal de A).

Démonstration C'est immédiat par application du théorème de Lagrange.

Proposition On suppose que G est fini. Soit $\{x_i; i = 1, \dots, n\}$ un sous ensemble d'éléments de X tel que $\{w(x_i); i = 1, \dots, n\}$ est une partition de X . Alors

$$|X| = \sum_{i=1}^n |w(x_i)| = |G| \sum_{i=1}^n (|\text{stab}(x_i)|)^{-1}.$$

Théorème Formule de la moyenne On suppose G de cardinal fini et agissant sur un ensemble X . Alors si n désigne le nombre d'orbites distinctes de l'action, si \mathcal{A} désigne le sous ensemble de X composé d'un représentant pour chacune de ces orbites, on a:

$$n = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Démonstration Considérons un sous ensemble \mathcal{A} de X comme dans l'énoncé du théorème. Nous allons nous intéresser à l'ensemble $G \times X$, et plus précisément au sous ensemble \mathcal{O} de ce dernier défini par $\mathcal{O} = \{(g, x) \in G \times X; g.x = x\}$. On a

$$\mathcal{O} = \bigcup_{g \in G} \{g\} \times \text{Fix}(g) = \bigcup_{x \in X} \text{Stab}(x) \times \{x\}.$$

Ceci nous donne:

$$\sum_{g \in G} |\text{Fix}(g)| = \sum_{x \in X} |\text{Stab}(x)|.$$

On a aussi:

$$\sum_{x \in X} |\text{Stab}(x)| = \sum_{i=1}^n \sum_{x \in w(x_i)} |\text{Stab}(x_i)|.$$

Mais pour tout $x \in X$, $|\text{stab}(x)|.|w(x)|=|G|$. Donc

$$\sum_{x \in X} |\text{Stab}(x)| =$$

5.3. PROPRIÉTÉS

$$\begin{aligned} \sum_{i=1}^n \sum_{x \in w(x_i)} \frac{|G|}{|w(x)|} &= \\ |G| \sum_{i=1}^n \sum_{x \in w(x_i)} \frac{1}{|w(x_i)|} &= \\ |G| \sum_{i=1}^n \left(\sum_{x \in w(x_i)} 1 \right) \cdot \frac{1}{|w(x_i)|} &= \\ |G| \sum_{i=1}^n |w(x_i)| \cdot \frac{1}{|w(x_i)|} &= n \cdot |G|. \end{aligned}$$

En divisant par $|G|$ les deux membres de notre égalité, on obtient la formule voulue.

Chapitre 6

Théorème de Cauchy et théorèmes de Sylow

Par Emmanuel Vieillard Baron

6.1 Introduction

Le théorème de Lagrange nous apprend que l'ordre d'un élément dans un groupe fini est un diviseur de l'ordre du groupe. Le théorème de Lagrange peut s'énoncer encore sous la forme suivante: l'ordre d'un sous groupe d'un groupe engendré par un élément de ce groupe est un diviseur de l'ordre du groupe. Il est alors naturel de se poser le problème de la réciproque:

- Si p est un diviseur de l'ordre d'un groupe existe-t-il un élément d'ordre p dans ce groupe?
- Si p est un diviseur de l'ordre d'un groupe, existe-t-il un sous groupe d'ordre p dans ce groupe?

Le théorème de Cauchy, puis ceux de Sylow qui sont une généralisation du premier, apporteront des éléments de réponse à ces questions.

6.2 Théorème de Cauchy

Théorème de Cauchy Soit (G, \cdot) un groupe fini et p un diviseur premier de l'ordre de G . Alors il existe un élément d'ordre p dans G .

Démonstration Soit p un diviseur premier de $|G|$. Considérons l'ensemble

$$X = \{(x_1, \dots, x_p) \in \underbrace{G \times \dots \times G}_{p \text{ fois}}; x_1 \cdot x_2 \cdot \dots \cdot x_p = e\}$$

où e désigne le neutre de G . Pour choisir un élément x de X , nous devons faire $p-1$ choix d'éléments dans G , donc le cardinal de X est $|G|^{p-1}$. On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X de la façon suivante: (*On commettra sans aucun scrupule l'abus de notation qui consiste*

6.3. THÉORÈMES DE SYLOW

à identifier la classe d'équivalence de $i \in \mathbb{Z}$ et l'élément de \mathbb{Z} compris entre 0 et $p-1$ qui est un représentant de cette classe d'équivalence. Autrement dit, on ne sera pas gêné par l'égalité $\bar{i}=k$ où k est le représentant de \bar{i} qui est compris entre 0 (compris) et p (non compris). Si x est l'élément (x_1, \dots, x_p) de X et si \bar{i} est la classe d'équivalence de i ($0 \leq i < p$) dans $\mathbb{Z}/p\mathbb{Z}$, alors $\bar{i}.x = (x_{1+i}, \dots, x_{p+i})$. On vérifie sans peine que ceci définit bien une action sur X . Supposons que G ne possède aucun élément d'ordre p . Remarquons que l'orbite de $(e, \dots, e) \in X$ n'a qu'un élément. Si un autre élément x de X n'a que lui-même dans son orbite, alors en particulier,

$$x = (x_{\bar{1}}, \dots, x_{\bar{p}}) = (x_{\bar{1+1}}, \dots, x_{\bar{p+1}}) = (x_2, \dots, x_p, x_1) = (x_3, \dots, x_1, x_2) = \dots$$

Et donc $x_1 = x_2 = \dots = x_p$ et $x_1^p = e$, ce qui implique que G possède un élément x_1 d'ordre p et est contraire à notre hypothèse de départ. On suppose donc que (e, \dots, e) est le seul élément de X possédant une orbite ne contenant que lui-même. Si x est un élément de X , $|w(x)|$ est alors un diviseur de $|\mathbb{Z}/p\mathbb{Z}| = p$ différent de 1. Comme p est premier, ceci implique que $|w(x)| = p$. Choisissons alors des éléments x de X dont les orbites respectives partitionnent X . La formule des classes nous donne:

$$|X| = |X^G| + \sum_{x \text{ partitionnant } X} |w(x)|.$$

Donc $|X|$ est de la forme $1+m.p$ où m désigne le nombre d'orbites de taille plus grande que 1 et partitionnant X . Ceci contredit le fait que $|X|$ est de cardinal $|G|^{p-1}$ qui est divisible par p . Nous venons alors de démontrer par l'absurde que G possédait au moins un élément d'ordre p .

6.3 Théorèmes de Sylow

Définition On dit que le groupe fini (G, \cdot) est un **p-groupe** si p est premier et si le cardinal de G est une puissance de p .

Proposition Si G est un p -groupe agissant sur un ensemble X et si $X^G = \{x \in X; \forall g \in G, g.x = x\}$ alors on a:

$$|X| \equiv |X^G| \pmod{p}$$

Démonstration Soient x_1, \dots, x_k des éléments de X tels que $\{X^G, w(x_1), \dots, w(x_k)\}$ définit une partition de X . X^G est en fait l'ensemble des éléments de X dont l'orbite est constituée d'un unique point. On suppose donc que pour tout $i=1, \dots, k$ $|w(x_i)| > 1$. Comme $|w(x_i)|$ est un diviseur de $|G| = p^\alpha$ et que p est premier, $|w(x_i)|$ est de la forme $p^{\alpha'}$ avec $\alpha' \geq 1$. Donc p divise $|w(x_i)|$ pour tout $i=1, \dots, k$. Mais comme X est la réunion disjointe des éléments de $\{X^G, w(x_1), \dots, w(x_k)\}$ alors son cardinal est la somme des cardinaux de tout ces éléments et comme p divise chaque $|w(x_i)|$, $|X| \equiv |X^G| \pmod{p}$.

Définition Soit G un groupe de cardinal $n = p^\alpha . m$ avec p premier et p ne divisant pas m . On dit que le sous groupe H de G est un **p-Sylow** de G si $|H| = p^\alpha$.

6.3. THÉORÈMES DE SYLOW

Voici un exemple de p-Sylow.

Proposition Soit le corps fini $\mathbb{F}^p \simeq \mathbb{Z}/p\mathbb{Z}$ (p est un nombre premier). Considérons l'ensemble des matrices inversibles de rang n à coefficient dans \mathbb{F}^p . Cet ensemble, noté $\text{GLn}(\mathbb{F}^p)$, est un groupe de cardinal $m \cdot p^{\frac{n(n-1)}{2}}$ où m et n sont des entiers non nuls. Si l'on note T le sous ensemble de $\text{GLn}(\mathbb{F}^p)$ des matrices triangulaires supérieures de rang n , à coefficients dans \mathbb{F}^p et à éléments diagonaux tous égaux à 1, alors T est un p-Sylow de $\text{GLn}(\mathbb{F}^p)$.

Démonstration On ne démontrera pas que $\text{GLn}(\mathbb{F}^p)$ est un groupe. Ceci est un résultat de base d'algèbre linéaire. On ne démontrera pas non plus que T est un sous groupe de $\text{GLn}(\mathbb{F}^p)$ car c'est relativement facile. Calculons par contre le cardinal de $\text{GLn}(\mathbb{F}^p)$. Etudions la première colonne d'une matrice de $\text{GLn}(\mathbb{F}^p)$. On peut choisir n'importe quelle valeur pour les éléments de cette colonne. La seule éventualité à éviter est que tout les éléments de cette colonne soient nuls simultanément. Cela nous fait donc $p^n - 1$ possibilités pour cette première colonne. Etudions maintenant la deuxième colonne. Les éléments de cette colonne peuvent prendre n'importe quelles valeurs. Les seules conditions à vérifier sont que cette colonne ne soit pas dépendante de la première et qu'elle ne soit pas nulle. Il y a $p-1$ colonnes possibles dépendantes de la première et qu'une colonne nulle possible. Cela nous fait alors $p^n - p$ possibilités pour la deuxième colonne. De même, par récurrence, on établit qu'il y a $p^n - p^k$ possibilités pour la $k^{\text{ième}}$ colonne. Donc $|\text{GLn}(\mathbb{F}^p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$. Ce cardinal peut se re-écrire sous la forme: $p \cdot p^2 \dots p^{n-1} \cdot (p^n - 1)(p^{n-1} - 1) \dots (p - 1) = p^{1+2+\dots+n-1} \cdot (p^n - 1)(p^{n-1} - 1) \dots (p - 1) = p^{\frac{n(n-1)}{2}} \cdot (p^n - 1)(p^{n-1} - 1) \dots (p - 1)$. Donc, en posant m égal à la partie du produit précédent qui est après le premier facteur, on vient de montrer que $|\text{GLn}(\mathbb{F}^p)| = m \cdot p^{\frac{n(n-1)}{2}}$. Calculons maintenant le cardinal de T . Pour cela remarquons qu'il y a p^{n-1} choix possibles pour la première ligne, p^{n-k} choix possibles pour la $k^{\text{ième}}$ ligne. Au total, cela nous fait $p \cdot p^2 \dots p^{n-1}$ choix possibles pour une matrice de T . Ceci prouve que $|T| = p^{\frac{n(n-1)}{2}}$ et que T est un p-Sylow de $\text{GLn}(\mathbb{F}^p)$.

Avant d'énoncer les théorèmes de Sylow, démontrons le lemme suivant qui nous sera fort utile pour la suite.

Lemme Soit G un groupe de cardinal n , p un diviseur premier de n tel que $n = p^\alpha \cdot m$ et p ne divisant pas m , soit H un sous groupe de G et S un p-sylow de G . Alors il existe g dans G tel que $g \cdot S \cdot g^{-1} \cap H$ soit un p-sylow de H .

Démonstration Considérons le quotient G/S qui est en fait l'ensemble des classes à gauche de G relativement au sous groupe S : $G/S = \{a \cdot H; a \in G\}$. G agit sur G/S par translation à gauche: $g \cdot aS = (ga)S$.

L'élément $g \in G$ est élément du stabilisateur de aS si et seulement si $g \cdot aS = aS$. C'est à dire si et seulement si g est élément de aSa^{-1} . Réciproquement, on montre que si g est élément de aSa^{-1} alors $g \in \text{Stab}(aS)$. H agit sur G/S par restriction de l'action de G . Le stabilisateur d'un élément aS pour cette nouvelle action est alors de la forme $aSa^{-1} \cap H$.

S étant un p-Sylow de G , $|S| = p^\alpha$. Comme aSa^{-1} est un sous groupe conjugué de

6.3. THÉORÈMES DE SYLOW

S , il a même cardinal que S . De plus, comme H est un sous groupe de G , son cardinal est, d'après le théorème de Lagrange, de la forme $m \cdot p^\alpha$ où m divise m et où $\alpha' \leq \alpha$. L'intersection de deux sous groupes d'un groupe est encore un sous groupe. Donc $aSa^{-1} \cap H$ est un sous groupe de G . C'est de plus un sous groupe de H et de S . Son cardinal, toujours d'après le théorème de Lagrange, divise à la fois p^α et $m \cdot p^{\alpha'}$. Il est donc de la forme $p^{\alpha''}$ où α'' est à la fois plus petit (ou égal) à α et à α' . Notons que α dépend à priori de a . Supposons que pour tout a dans G , $\alpha''(a) < \alpha'$. Cette hypothèse revient à supposer que $aSa^{-1} \cap H$ n'est jamais un p -Sylow de H . Alors, comme l'orbite d'un élément aS de G/S par l'action de H vérifie la formule $|w(aS)| = |H|/|\text{Stab}(aS)|$ et que $\text{Stab}(aS) = aSa^{-1} \cap H$, on a $|w(aS)| = m \cdot p^{\alpha' - \alpha''}$. Comme pour tout a de G , on a supposé que $\alpha''(a) < \alpha'$ alors p divise $|w(aS)|$ et ce $\forall a \in G$.

Mais $\{w(aS); a \in G\}$ définit une partition de G/S . La réunion de toutes ces orbites est égale à G/S . Le cardinal de G/S est donc divisible par p . Mais ceci est impossible car d'après le théorème de Lagrange $|G/S| = m$ qui n'est pas divisible par p .

Nous avons donc abouti à une contradiction. Ceci nous permet d'affirmer qu'il existe un élément a de G tel que $aSa^{-1} \cap H$ est un p -Sylow de H .

Théorème (Premier théorème de Sylow) Si G est un groupe de cardinal n et que n vérifie $n = p^\alpha \cdot m$ avec p premier et p ne divisant pas m , alors G possède un p -Sylow.

Démonstration Soit G un groupe comme dans l'énoncé du théorème. Le théorème de Cayley nous permet d'affirmer l'existence d'un morphisme injectif de G dans le groupe symétrique à n éléments S_n . Mais on a une injection évidente de S_n dans $\text{GL}_n(\mathbb{F}^p)$: à toute permutation ϕ de S_n , on fait correspondre l'application linéaire f définie par : si $(e_i)_{i=1..n}$ est une base de $(\mathbb{F}^p)^n$ alors $f(e_i) = e_{\phi(i)}$. On réalise ainsi une injection de G dans $\text{GL}_n(\mathbb{F}^p)$. Ainsi, l'image d'un groupe par un morphisme étant un sous groupe du groupe d'arrivée du morphisme, et notre morphisme étant injectif (et surjectif sur son image) G est isomorphe à un sous groupe H de $\text{GL}_n(\mathbb{F}^p)$. De plus, comme on l'a vu dans l'exemple précédent, $\text{GL}_n(\mathbb{F}^p)$ possède un p -Sylow S . D'après le lemme précédent, il existe alors un élément a de $\text{GL}_n(\mathbb{F}^p)$ tel que $aSa^{-1} \cap H$ est un p -Sylow de H . H contient donc un p -Sylow. Ce p -Sylow se transporte par l'application inverse de notre isomorphisme vers un p -Sylow du groupe G . Cqfd.

Théorème Soit G un groupe de cardinal n , n vérifiant $n = p^\alpha \cdot m$ avec p premier et p ne divisant pas m . G contient, d'après le premier théorème de Sylow, un ou des p -Sylow.

- (**Second théorème de Sylow**) Les p Sylow de G sont tous conjugués. De plus, leur nombre k divise n .
- (**Troisième théorème de Sylow**) Le nombre k de p -Sylow dans G vérifie : $k \equiv 1 \pmod{p}$.

Démonstration Considérons $\mathcal{A} = \{S_1, \dots, S_k\}$ l'ensemble des p Sylow de G . D'après le premier lemme de ce paragraphe, pour tout $i=1..k$, il existe un élément a de G tel que $aS_1a^{-1} \cap S_i$ soit un p -Sylow de S_i . Mais en raison de ce fait et des cardinaux respectifs de aS_1a^{-1} et de S_i , on en déduit que $aS_1a^{-1} = S_i$. On démontre ainsi que tous les p -Sylow sont conjugués.

Remarquons à ce stade de la démonstration que si un p -Sylow est normal dans le groupe qui le contient, alors nécessairement, il est l'unique p -Sylow de ce groupe.

6.3. THÉORÈMES DE SYLOW

Faisons maintenant agir G par conjugaison sur \mathcal{A} : $g.S_i = gS_i g^{-1}$. Cette action est, avec ce qui vient d'être établi, bien définie. De plus, comme tous les p -syloves de G sont conjugués, cette action n'engendre qu'une et une seule orbite sur \mathcal{A} . Comme le cardinal de l'orbite d'un point par une action est un diviseur du cardinal du groupe définissant cette action, on en déduit que k est un diviseur du cardinal de G .

S_1 agit de même sur \mathcal{A} par restriction de l'action de G sur \mathcal{A} .

Étudions le sous-ensemble \mathcal{A}^{S_1} de \mathcal{A} . S_i est un élément de \mathcal{A}^{S_1} si et seulement si pour tout g de S_1 , $g.S_i.g^{-1}$ est inclus dans S_i . Si on considère le sous-groupe H de G engendré par S_i et S_1 , on en déduit que $S_i \triangleleft H$. Mais S_i et S_1 sont deux p -Syloves de H . Donc, d'après la remarque faite précédemment, ceci implique que ces deux p -Syloves n'en forment qu'un: $S_1 = S_i$. Le seul p -Sylove contenu dans \mathcal{A}^{S_1} est donc S_1 . Mais S_1 est un p groupe. Donc d'après la proposition établie tout au début de ce thème, $|\mathcal{A}| \equiv |\mathcal{A}^{S_1}| \equiv 1 \pmod{p}$. Donc $k \equiv 1 \pmod{p}$, Cqfd.

Voici un corollaire immédiat de ce qui vient d'être démontré.

Corollaire Soit G un groupe de cardinal n , n vérifiant $n = p^\alpha \cdot m$ avec p premier et p ne divisant pas m . Soit k le nombre de p -Syloves dans G . Alors k divise m et k est premier avec p .

Démonstration Cela découle directement des deux théorèmes précédents.

Remarquons avant d'en terminer avec ce thème que le premier théorème de Sylow implique le théorème de Cauchy.