Groupes

Christian CYRILLE

19 janvier 2019

Dédicacé à mon ami Albert BERGER en souvenir de notre préparation aux oraux de l'Agrégation.

"Quand vous doutez, cherchez le groupe"
André WEIL

Évariste Galois (Bourg-la-Reine, 25 octobre 1811 – Paris, 31 mai 1832)

est un mathématicien français. Il a entre autres laissé son nom à la théorie de Galois, qui étudie la résolubilité des équations algébriques à partir des groupes de permutations de leurs racines et qui est considérée comme un ingrédient important dans le point de vue structural des mathématiques modernes. Il a aussi contribué à l'élaboration des « corps de Galois », autre nom des corps finis, qui jouent par exemple un rôle essentiel en cryptographie. Les démêlés de Galois avec les autorités, tant scientifiques que politiques, les zones d'ombre entourant sa mort prématurée, contrastant avec l'importance reconnue maintenant à ses travaux, ont contribué à en faire l'incarnation même du génie malheureux. L'année 2011, bicentenaire de sa naissance, sera l'occasion de multiples manifestations.
Évariste Galois naquit le 25 octobre 1811 à Bourg-la-Reine. C'était le deuxième enfant de Nicolas-Gabriel Galois, qui devint maire de Bourg-la-Reine en 18153, et de Adélaïde-Marie Demante, issue d'une famille de juristes.
Il intégra en 1823 le collège Louis-le-Grand en classe de quatrième et obtint tout d'abord des prix en latin et en grec. Néanmoins, il redoubla sa seconde et, suite à une réforme pédagogique, suivit des cours de mathématiques qui le passionnèrent ; il commença à lire directement les travaux des mathématiciens, en particulier les Éléments de géométrie de Legendre, les traités algébriques et analytiques de Lagrange, les Recherches arithmétiques de Gauss.
En 1826, Galois obtint un prix en mathématiques au concours général et, l'année suivante, l'un de ses professeurs déclara à son sujet : « C'est la fureur des mathématiques qui le domine ; aussi je pense qu'il vaudrait mieux pour lui que ses parents consentent à ce qu'il ne s'occupe que de cette étude ». Galois décida de se présenter dès l'été 1828 au concours d'entrée à l'École polytechnique, sans être passé comme il était d'usage par une classe de mathématiques spéciales, et y échoua une première fois.
En 1829, toujours élève de Louis-le-Grand, cette fois dans la classe de Louis-Paul-Émile Richard qui reconnut son talent, il publia en mars dans les Annales de mathématiques pures et appliquées de Gergonne son premier article, portant sur le développement en fractions continues des racines d'un polynôme, et proposa ses premiers mémoires sur la théorie des équations à l'Académie des sciences le 25 mars et le 1er juin (voir description ci-dessous). Il se présenta cette année-là à la fois à l'École préparatoire, ancien nom de l'École normale supérieure (rue d'Ulm), et à l'École polytechnique. Le suicide de son père, Nicolas-Gabriel

Galois, le 2 juillet 1829, à la suite d'attaques politiques, précéda de peu son deuxième échec à l'entrée de cette dernière.
Galois entra alors à l'École préparatoire. Il obtint en décembre ses deux baccalauréats (nécessaires pour valider son admission) et, comme tous les élèves de l'École, signa un engagement de dix ans avec l'Université, en février 1830. Dans les mois qui suivirent, il soumit deux nouveaux articles sur la théorie des équations, ainsi qu'un article sur la théorie des nombres dans le Bulletin de Férussac ; ces articles furent publiés en 1830. Selon la légende, le rapporteur des premiers mémoires, à savoir Cauchy, les aurait égarés. Mais certains historiens des mathématiques, comme René Taton et Tony Rothman (en), estiment plus vraisemblable que Cauchy aurait refusé de les présenter pour que Galois puisse soumettre au Grand Prix des sciences mathématiques de 1830 un mémoire, révisé, sur la résolubilité des équations algébriques ; mais le Prix échut à Abel (à titre posthume) et à Jacobi. Le manuscrit de Galois avait été envoyé à Fourier, qui mourut en mai ; le mémoire fut annoncé perdu. Selon un article publié dans le journal Le Globe en juin 1831, Cauchy aurait pourtant mentionné aux membres du jury son intérêt pour les travaux de Galois : « M. Cauchy avait à ce sujet prodigué les plus grands éloges à son auteur ».
La Révolution de juillet 1830 marqua le début de son engagement politique du côté républicain. Les élèves de l'École préparatoire (dont Galois) furent enfermés pour les empêcher de prendre part à l'insurrection parisienne. À la rentrée, la direction de l'École repoussa leur demande d'avoir des armes et de « s'exercer aux manœuvres militaires, afin de pouvoir défendre le territoire, en cas de besoin ». Un texte acerbe contre le directeur de l'École, Guigniault, publié dans la Gazette des Écoles, conduisit en décembre 1830 à l'expulsion de Galois, qui venait d'obtenir sa licence. À la même période, il semble s'être engagé dans la Société des Amis du Peuple, dont faisait partie l'artillerie de la Garde nationale et se consacra dès lors très activement au combat politique.
Galois soumit un autre mémoire à l'Académie sur la résolution des équations polynomiales en janvier 1831. Il ouvrit aussi un cours public d'algèbre supérieure, dont une seule séance semble s'être tenue. En mai, aux « Vendanges de Bourgogne », un restaurant de Belleville, au cours d'un banquet organisé pour l'acquittement d'officiers républicains accusés d'avoir disposé d'armes (dont Pescheux d'Herbinville), Galois porta un toast « à Louis-Philippe », mais avec un couteau à la main au-dessus de son verre. Arrêté, il passa un mois en prison avant d'être jugé et acquitté11. Galois fut de nouveau arrêté le 14 juillet 1831 pour port illégal de l'uniforme de l'artillerie ; jugé le 23 octobre, il fut condamné cette fois à six mois de prison ; enfermé à Sainte-Pélagie, il y côtoya François-Vincent Raspail qui le décrit dans ses Lettres sur les prisons de Paris, et Gérard de Nerval. D'après son ami et condisciple de l'École normale, Auguste Chevalier (1809-1868), le mémoire de 1831 aurait été soumis à la demande de Siméon Denis Poisson, mais celui-ci le refusa le 4 juillet ; le mémoire lui semblant difficile à évaluer et Galois y ayant annoncé une théorie plus vaste, Poisson suggérait d'attendre la publication de cette dernière : « il arrive que les différentes parties d'une théorie, en s'éclairant mutuellement, sont plus faciles à saisir dans leur ensemble qu'isolément ». En prison, Évariste Galois réussit néanmoins à travailler ses mémoires sur les équations et à entamer d'autres recherches sur les fonctions elliptiques.
En mars 1832, Galois fut transféré dans une clinique privée à cause d'une épidémie de choléra. Il semble y avoir rencontré une jeune femme, qui pourrait être

Stéphanie Poterin du Motel, et dont il s'éprit d'un amour apparemment malheureux. Elle lui demanda de rompre le 14 mai. Quelques semaines plus tard, le 30 mai 1832, il affronta en duel Pescheux d'Herbinville (ou Ernest Duchâtelet). Blessé à l'abdomen, Galois fut transporté à l'hôpital Cochin et mourut le 31 mai 1832, à l'âge de 20 ans et 7 mois, probablement d'une péritonite, après avoir refusé les offices d'un prêtre. Le Précurseur de Lyon publie un compte rendu détaillé de la mort d'Évariste, apportant ces précisions : « Le pistolet étant l'arme choisie par les deux adversaires, ils ont trouvé trop dur pour leur ancienne amitié d'avoir à viser l'un sur l'autre et ils s'en sont remis à l'aveugle décision du sort. À bout portant, chacun d'eux a été armé d'un pistolet et a fait feu. Une seule de ces armes était chargée. »
La veille du duel, le 29 mai, il avait rédigé plusieurs lettres adressées à Napoléon Lebon, Vincent Delaunay (des amis républicains) et surtout à Auguste Chevalier. Cette dernière, restée célèbre, est souvent décrite comme son testament mathématique : Galois enjoint à son ami de « prier publiquement Jacobi ou Gauss de donner leur avis, non sur la vérité, mais sur l'importance des théorèmes » qu'il a trouvés et dont il dresse le bilan, et de faire imprimer la lettre dans la Revue encyclopédique, ce que Chevalier fit en septembre 1832. Galois fut enterré le 2 juin 1832 au cimetière du Montparnasse à Paris en présence de deux à trois mille républicains.
Les papiers d'Évariste Galois, rassemblés par Chevalier et son jeune frère Alfred, furent soumis à Joseph Liouville qui recommanda à l'Académie des sciences son principal résultat de la théorie des équations algébriques obtenu en septembre 1843. Liouville fit ensuite publier les travaux de Galois en 1846 dans son journal, le Journal de mathématiques pures et appliquées, ce qui leur conféra aussitôt un rayonnement international.
Source : Paul Dupuy, « La vie d'Évariste Galois », dans Annales scientifiques de l'École normale supérieure, 3e série, no 13, 1896, p. 197-266 Rééd. Paris, Gabay, 1992. Incluant des pièces justificatives en fac-similé, cette étude est la principale source biographique sur Galois.

Table des matières

Chapitre 1

Généralités sur les groupes

1.1 Définition d'un magma

On appelle magma tout couple $(E, *)$ où $*$ est une loi de composition interne c'est-à-dire une application de $E \times E$ dans E.

1.2 Définition d'un semi-groupe

Soit un ensemble G muni d'une loi de composition interne $*$.
On dit que $(G, *)$ est un semi-groupe lorsque :

1. $*$ est associative.
2. G admet un élément neutre pour $*$ c'est-à-dire

$$\exists e \in G \ \forall x \in G \quad x * e = e * x = x$$

Par exemple, $(\mathbb{N}, +)$ est un semi-groupe.

1.3 Définition d'un groupe

Soit un ensemble G muni d'une loi de composition interne $*$.
On dit que $(G, *)$ est un groupe lorsque :

1. $*$ est associative.
2. G admet un élément neutre pour $*$ c'est-à-dire

$$\exists e \in G \ \forall x \in G \quad x * e = e * x = x$$

3. tout élément x de G admet un symétrique pour $*$ **dans** G c'est-à-dire

$$\forall x \in G \ \exists x' \in G \quad x * x' = x' * x = e$$

Si de plus, $*$ est commutative , on dit alors que le groupe $(G, *)$ est commutatif ou abélien(du nom du mathématicien ABEL).
Exemples : $(\mathbb{Z}, +); (\mathbb{Q}, +); (\mathbb{R}, +); (\mathbb{R}^*, \times)$

Niels Henrik Abel, né le 5 août 1802 à Frindoë près de Stavanger et mort le 6 avril 1829 (à 26 ans) à Froland près d'Arendal , est un mathématicien norvégien. Il est connu pour ses travaux en analyse mathématique sur la semi-convergence des séries numériques, des suites et séries de fonctions, les critères de convergence d'intégrale généralisée, sur la notion d'intégrale elliptique ; en algèbre, sur la résolution des équations.

1.3.1 Remarque

Dans la pratique, pour démontrer que l'on a une structure de groupe, on cherche d'abord à prouver la commutativité de $*$, ce qui allège les démonstrations de l'existence de l'élément neutre car $x * e = e * x$ et celle de l'existence d'un élément symétrique car $x * x' = x' * x$

1.4 Propriétés

1.4.1 Théorème

L'élément neutre d'un groupe G s'il existe est unique.

Démonstration

On raisonne par l'absurde.
Supposons qu'il y ait deux éléments neutre e et e' alors

1. e est l'élément neutre donc $\forall x \in G \quad x * e = e * x = x$.
   En prenant $x = e'$ on obtient $e' * e = e * e' = e'$
2. e' est l'élément neutre donc $\forall x \in G \quad x * e' = e' * x = x$.
   En prenant $x = e$ on obtient $e * e' = e' * e = e$
3. Par conséquent $e = e * e' = e'$ CQFD.

1.4.2 Théorème

Si un élément x de G admet un symétrique x' dans G alors ce symétrique x' est unique.

Démonstration

On raisonne par l'absurde.
Supposons que x a deux éléments symétriques x' et $x"$ alors

1. x a pour symétrique x' donc $x * x' = x' * x = e$.
2. x a pour symétrique $x"$ donc $x * x" = x" * x = e$.
3. Par conséquent en utilisant le fait que e est le neutre et le fait que $*$ soit associative on a

$$x' = x' * e = x' * (x * x") = (x' * x) * x" = e * x" = x".$$

CQFD.

1.4.3 Théorème

Si x et y sont des éléments d'un groupe $(G, *)$ de symétriques respectifs x' et y' alors $x * y$ a pour symétrique $y' * x'$.

Démonstration

$x*y*y'*x' = x*(y*y')*x' = x*e*x' = x*x' = e$ donc $x*y$ a pour symétrique $y' * x'$.

1.4.4 Théorème

Tout élément d'un groupe est régulier c'est-à-dire

1. $\forall (x, y, z) \in G^3 \qquad x * y = x * z \Longrightarrow y = z$ (régularité à gauche)
2. $\forall (x, y, z) \in G^3 \qquad y * x = z * x \Longrightarrow y = z$ (régularité à droite)

On peut "simplifier" par x à gauche et à droite.

1.4.5 Axiomes affaiblis d'un groupe

Soit un ensemble G muni d'une loi de composition interne $*$ telle que

1. $*$ est associative.
2. G admet un élément neutre à gauche pour $*$ c'est-à-dire

$$\exists e \in G \qquad \forall x \in G \qquad e * x = x$$

3. tout élément x de G admet un symétrique à gauche pour $*$ **dans** G c'est-à-dire

$$\forall x \in G \qquad \exists x' \in G \qquad x' * x = e$$

Alors $(G, *)$ est un groupe

1.4.6 Ordre d'un groupe

- L'ordre d'un groupe G est le cardinal de son ensemble sous-jacent. Il se note $ord(G), |G|$ ou $\#G$.
- Le groupe G est dit **fini ou infini** suivant que son ordre est fini ou infini.

1.4.7 Création de tables de CAYLEY de lois de groupes finis

Arthur CAYLEY 1821-1895

Remarques

- On désigne par e l'élément neutre et on peut alors remplir immédiatement la ligne et la colonne de e : $a \star e = a; b \star e = b \cdots$
- R_1 : : on ne peut pas avoir 2 fois le même élément dans une même ligne ou une même colonne.
  En effet, si dans la colonne de c, on trouvait a en ligne b et en ligne d alors $b \star c = a$ et $d \star c = a$ d'où $b \star c = d \star c$ donc par régularité on aurait $b = d$. Or $b \neq d$ puisque l'on veut construire un groupe d'éléments distincts deux à deux.
- Quand la table de la loi est construite, alors
  — Si la table est symétrique par rapport à la diagonale principale alors la loi $\star$ est commutative.
  — e est élément neutre par construction.
  — On vérifie que chaque élément a un symétrique. Bien entendu e est son propre symétrique.
  — On vérifie que la loi $\star$ est associative :
  $\forall (x, y, z \in G^3 \quad (x \star y) \star z = x \star (y \star z)$.
  R_2 : Cette égalité est automatiquement vérifié dans le cas où e est l'un des trois éléments x, y, z car
  — $(e \star y) \star z = y \star z = e \star (y \star z)$
  — $(x \star e) \star z = x \star z = x \star (e \star z)$
  — $(x \star y) \star e = x \star y = x \star (y \star e)$
  R_3 : Cette égalité est automatiquement vérifiée lorsque la loi est commutative dans le cas où l'on prend 3 fois le même élément :
  $(x \star x) \star x = x \star (x \star x)$

Groupe à 1 élément

Un groupe est forcément non vide car il contient son élément neutre e.
Un ensemble formé d'un seul élément $\{e\}$ peut être muni d'une structure de groupe en créant la loi interne $e \star e = e$.

$\star$	e
e	e

$\star$ est commutative. $\star$ est commutative d'après R_3 car on ne peut prendre que 3 fois l'élément e.
Il n'y a donc qu'un seul modèle de groupe de cardinal 1 : aussi tous les groupes de cardinal 1 sont isomorphes.
Ce groupe est cyclique car G est engendré par e donc $G =< e >$.

Groupes à 2 éléments

Un ensemble de 2 éléments $\{e\ ;\ a\}$ peut être muni d'une structure de groupe : l'un de ses éléments est l'élément neutre e et l'autre a est son propre symétrique. La table de la loi interne qui convient est :

$\star$	e	a
e	e	a
a	a	e

La table est symétrique donc $\star$ est commutative alors $\star$ sera associative d'après R_2 et R_3 car on ne peut prendre que 3 fois a ou au moins une fois e.
Il n'y a donc qu'un seul modèle de groupe de cardinal 2 : aussi tous les groupes de cardinal 2 sont isomorphes.
Ce groupe est cyclique car G est engendré par a donc $G = \{e; a\} =< a >$

Groupes à 3 éléments

Un ensemble de 3 éléments $\{e\ ;\ a\ ;\ b\}$ peut être muni d'une structure de groupe :

- l'un de ses éléments est l'élément neutre e
- le deuxième a ne peut être son propre symétrique
  car si c'était le cas , on aurait $a^2 = e$ mais alors $ab \neq e$ car l'inverse de a est déjà a. Or $ab \neq a$ sinon cela entrainerait que $b = e$
- Donc le groupe a comme éléments e, a et $y = a^2$

La table de la loi interne qui convient est :

$\star$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

1. Cette table est symétrique donc $\star$ est commutative.
2. Par conséquent, d'après R_2 et R_3 la propriété d'associativité est vérifiée si l'on prend 3 fois le même élément ou si l'un des 3 éléments est e
3. Reste à vérifier l'associativité si l'on prend 2 fois a et une fois b ou 1 fois a et 2fois b. Mais comme $\star$ est commutative, il suffit de le vérifier pour 2 fois a et 1 fois b :

   - $(b \star a) \star a = e \star a = a$ et $b \star (a \star a) = b \star b = a$
   - $(a \star b) \star a = e \star a = a$ et $a \star (b \star a) = a \star e = a$
   - $(a \star a) \star b = b \star b = a$ et $a \star (a \star b) = a \star e = a$

Il n'y a donc qu'un seul modèle de groupe de cardinal 3 : aussi tous les groupes de cardinal 3 sont isomorphes.
Ce groupe est cyclique engendré par tout élément non neutre.

- $G =< a >$ car $a \star a = b; a \star a \star a = b \star a = e$
- $G =< b >$ car $b \star b = a; b \star b \star b = a \star b = e$

Groupes à 4 éléments

Un ensemble de 4 éléments $\{e\ ;\ a\ ;\ b\ ;\ c\}$ peut être muni d'une structure de groupe :

- **ou bien il y a un élément a qui n'est pas son propre symétrique :**
  Cet élément $a \neq e$ car e est son propre symétrique. On pose b le symétrique de a alors $a * b = b * a = e$.
  $b \neq a$ car a n'est pas son propre symétrique.
  $b \neq e$ sinon $e = a * b = a * e = a$ impossible.
  a et b sont symétriques l'un de l'autre donc c est son propre symétrique.
  La table de la loi interne qui convient est :

$\star$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

  Cette table est symétrique donc $\star$ est commutative.
  On démontre l'associativité en étudiant tous les cas sauf ceux déjà prévus par R_2 et R_3.
  On vérifie que cette table définit une structure de groupe commutatif appelé **le groupe du carré** par analogie au groupe,des rotations conservant un carré.
  On aura donc 2 éléments qui sont leur propre symétrique(dont e) et deux autres qui ne sont pas leurs propres symétriques.
  Ce type de groupe est cyclique car il est engendré par tout élément qui n'est pas son propre symétrique :
  — $G =< a >$ car $a \star a = c; a \star a \star a = b; a \star a \star a \star a = b \star a = e$
  — $G =< b >$ car $b \star b = c; b \star b \star b = a; b \star b \star b \star b = a \star b = e$
  — $G \neq< c >= \{e; c\}$
  — $G \neq< e >= \{e\}$
- **ou bien chaque élément est son propre symétrique :**
  La table de la loi interne qui convient est :

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

  Le produit de deux éléments non neutres est le troisième élément non neutre.
  Cette table est symétrique donc $\star$ est commutative.
  On démontre l'associativité en étudiant tous les cas sauf ceux déjà prévus par R_2 et R_3 ;
  On vérifie que cette table définit une structure de groupe commutatif appelée **Groupe de KLEIN.**.
  Un groupe de KLEIN n'est pas cyclique car :
  $< a >= \{e; a\}; < b >= \{e; b\}; < c >= \{e; c\}; < e >= \{e\}$

- Il y a donc 2 modèles de groupes d'ordre 4 qui sont tous deux commutatifs.

1.4.8 Autres exemples de groupes

- $(\mathbb{Z}, +)$ est un groupe commutatif.
- $(\mathbb{Q}, +)$ est un groupe commutatif.
- $(\mathbb{R}, +)$ est un groupe commutatif.
- $(\mathbb{C}, +)$ est un groupe commutatif.
- $(\mathbb{Q} - \{0\}, \times)$ est un groupe commutatif.
- $(\mathbb{R} - \{0\}, \times)$; est un groupe commutatif.
- $(\mathbb{C} - \{0\}, \times)$ est un groupe commutatif.
- $(\mathcal{P}(E), \Delta)$ est un groupe commutatif car la différence symétrique est commutative, associative.
  De plus,$\mathcal{P}(E)$ admet $\emptyset$ pour élément neutre et toute partie A de E est son propre symétrique.

1.5 Sous groupes

1.5.1 Définition

Soit $(G, *)$ un groupe et soit H une partie non vide de G.
On dit que H est un sous-groupe de G ce que l'on note $H < G$ si

1. H est stable par $*$
2. H muni de la loi induite par $*$ a une structure de groupe

1.5.2 Propriété

L'élément neutre d'un sous groupe est l'élément neutre du groupe à cause de l'unicité de l'élément neutre dans un groupe.

1.5.3 Remarque

Si l'élément neutre e d'un groupe G n'appartient pas à H alors H ne peut être un sous groupe de G.

1.5.4 Théorème caractéristique 1

$$H \text{ est un sous-groupe de } G \iff \begin{cases} H \neq \emptyset \\ \forall (x,y) \in H^2 \; x * y \in H \\ \forall x \in H \text{ son symétrique } x' \in H \end{cases}$$

1.5.5 Théorème caractéristique 2

$$H \text{ est un sous-groupe de } G \iff \begin{cases} H \neq \emptyset \\ \forall (x,y) \in H^2 \; x * y' \in H \end{cases}$$

1.5.6 Remarque

Pour démontrer que $H \neq \emptyset$ il est astucieux de prouver que l'élément neutre e du groupe G appartient à H.
Car si cet élément neutre de G n'est pas dans H alors H ne peut-être un sous-groupe de G.

1.5.7 Propriété

Si $K < H$ et $H < G$ alors $K < G$

1.5.8 Propriété

Si $H_1 < G$ et $H_2 < G$ alors $(H_1 \cap H_2) < G$

Démonstration

évidente.

1.5.9 Sous-groupes triviaux, Centre, Centralisateur, Normalisateur

Soit $(G, .)$ un groupe d'élément neutre e, alors

1. G et $\{e\}$ sont des sous-groupes appelés sous-groupes triviaux de G.
2. Le centre de g noté
   $Z(G) = \{x \in G \ / \ \forall g \in G \quad xg = gx\}$ est un sous-groupe de G
3. Soit $A \subset G$.
   Le centralisateur de A dans G noté
   $C_G(A) = \{x \in G \ / \ \forall a \in A \quad xa = ax\}$ est un sous-groupe de G.
   On remarque que $C_G(G) = Z(G)$
4. Soit $B \subset G$.
   Le normalisateur de B dans G noté
   $N_G(B) = \{x \in G \ / \ xBx^{-1} = B\}$ est un sous-groupe de G.
   On remarque que $N_G(\{y\}) = Z(\{y\})$

1.5.10 Sous groupe engendré par une partie

Si G est un groupe d'élément neutre e , si $A \subset G$ et $A \neq \emptyset$.
L'ensemble des sous-groupes de G contenant A est non vide car il contient déjà G.
L'intersection de tous les sous-groupes contenant A est le plus petit sous-groupe contenant A.
On dit que c'est le sous-groupe engendré par A qu'on note $< A >$.
Par convention, $< \emptyset >= \{e\}$

Théorème

Si l'on note $A^{-1} = \{a^{-1}/a \in A\}$ l'ensemble des éléments symétriques des éléments de A.
Soit $B = A \cup A^{-1}$
alors $< A >= \{\prod_{k=1}^{n} a_i \quad /a_i \in B\}$ = l'ensemble des produits finis d'éléments de B

Théorème

1. Dans un groupe additif $(G, +)$ si $A = \{a\}$
   alors $< A >= \{na \quad /n \in \mathbb{Z}\}$
   $< A >= \{\cdots, -4a, -3a, -2a, -a, 0, a, 2a, 3a, 4a, \cdots\}$
2. Dans un groupe multiplicatif $(G, \times)$ si $A = \{a\}$
   alors $< A >= \{a^n \quad /n \in \mathbb{Z}\}$
   $< A >= \{\cdots, a^{-3}, a^{-2}, a^{-1}, a, a^2, a^3, a^4, \cdots\}$

1.5.11 Propriété

Attention ! ! ! la réunion de sous-groupes de G n'est pas en général un sous-groupe de G.
Il n'y a qu'une seule condition :
Si $H_1 < G$ et $H_2 < G$ alors :
$(H_1 \cup H_2) < G \iff H_1 \subset H_2$ *ou* $H_2 \subset H_1$.

Démonstration

1. $\Longleftarrow$:
   Supposons par exemple que $H_1 \subset H_2$ alors $H_1 \cup H_2 = H_2$ donc est un sous-groupe de G. CQFD.
2. $\Longrightarrow$:
   Démontrons que la contraposée à savoir que si H_1 n'est pas inclus dans H_2 et si H_2 n'est pas inclus dans H_1 alors $H_1 \cup H_2$ ne peut être un sous-groupe de G.

Comme H_1 n'est pas inclus dans H_2 et que H_2 n'est pas inclus dans H_1 alors $\exists a \in H_1$ et $a \notin H_2$ et $\exists b \in H_2$ et $a \notin H_1$. On a bien sûr $a \in H_1 \cup H_2$ et $b \in H_1 \cup H_2$. Mais $ab \notin H_1 \cup H_2$. Ce qui fait que $H_1 \cup H_2$ ne peut être un sous-groupe.
En effet si $ab = \alpha \in H_1$ alors $b = a^{-1}\alpha \in H_1$ car $\alpha \in H_1$ et le symétrique de a : $a^{-1} \in H_1$. Ce qui est impossible.

1.5.12 Théorème de Lagrange

♡ ♡ ♡ Si G est un groupe fini et H est un sous groupe de G alors H est fini et l'ordre de H divise l'ordre de G.

Démonstration

1. Soit la relation binaire $\mathcal{R}_H$ sur G par

$$\forall (x,y) \in G^2 \quad x \ \mathcal{R}_H \ y \iff x^{-1}.y \in H \iff y \in xH$$

   (a) $\mathcal{R}_H$ est une relation d'équivalence sur G car
   - $\forall x \in G \quad x^{-1}.x = 1 \in H$ car $H < G$ donc $x\mathcal{R}_H x$.
     $\mathcal{R}_H$ est donc réflexive.
   - $\forall (x,y) \in G^2$ si $x\mathcal{R}_H y$ alors $x^{-1}.y \in H$.
     En effet, le symétrique d'un élément d'un sous-groupe est encore dans ce sous-groupe donc $(x^{-1}.y)^{-1} = y^{-1}.(x^{-1})^{-1} = y^{-1}.x \in H$ donc $y\mathcal{R}_H x$.
     Donc $\mathcal{R}_H$ est symétrique.
   - $\forall (x,y,z) \in G^3$ si $x\mathcal{R}_H y$ et $y\mathcal{R}_H z$ alors $x^{-1}.y \in H$ et $y^{-1}.z \in H$.
     En effet, la composée de deux éléments d'un sous-groupe est encore dans ce sous-groupe donc $x^{-1}.y.y^{-1}.z \in H$ d'où $x^{-1}.z \in H$ donc $x\mathcal{R}_H z$. Donc $\mathcal{R}_H$ est transitive.

   (b) Soit $x \in G$ alors la classe modulo $\mathcal{R}_H$ de x est
   $\{y \in G \ / x \ \mathcal{R}_H \ y\} = \{y \in G \ / x^{-1}.y \in H\}$
   $= \{y \in G \ / \exists h \in H \quad x^{-1}.y = h\} = \{y \in G \ / \exists h \in H \quad y = x.h\}$
   donc c'est la partie $xH = \{x.h / h \in H\}$.
   On appelle $x.H$ la classe à droite modulo H de x.

   (c) Toute classe modulo $\mathcal{R}_H$ est en bijection avec H.

   (d) A quelle condition sur $x \in G$ la partie $x.H$ est-elle une groupe de G ?

2. On suppose maintenant G fini d'ordre n. Soit H un sous-groupe de G.

   (a) Justifier que H est un groupe fini. On note alors p son ordre. Que peut-on dire de p ?

   (b) Déduire des résultats du 1°) que toutes les classes modulo $\mathcal{R}_H$ sont toutes de cardinal p.

   (c) Pourquoi peut-on affirmer que le nombre de classes modulo $\mathcal{R}_H$ c'est-à-dire le nombre d'éléments de $\dfrac{G}{\mathcal{R}_H}$ est fini ?
   Soit q ce nombre. Que peut-on dire de ce nombre par rapport à n ?

   (d) Montrer que $Card(G) = Card(H)Card(\dfrac{G}{\mathcal{R}_H})$ c'est-à-dire que $n = pq$.

Application

> Il n'y a pas de sous-groupe dans $(\frac{\mathbb{Z}}{7\mathbb{Z}};+)$ autre que $\{\dot{0}\}$ et $\frac{\mathbb{Z}}{7\mathbb{Z}}$ lui-même car 7 est premier et n'a comme diviseurs positifs que 1 et 7

1.5.13 Caractérisation des sous groupes de $(\mathbb{Z}, +)$

♡ ♡ ♡ Les seuls sous groupes du groupe $(\mathbb{Z}, +)$ sont les $(n\mathbb{Z}, +)$ où $n \in \mathbb{N}$

Démonstration

1. On sait déjà que tous les $n\mathbb{Z}$ sont des sous groupes de $(\mathbb{Z}, +)$.
2. Reste donc à prouver que si H est un sous groupe de $(\mathbb{Z}, +)$ alors $\exists n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.
   (a) **unicité de** n :
   Supposons que $H = n\mathbb{Z}$ et que $H = n'\mathbb{Z}$ où $(n, n') \in \mathbb{N}^2$.
   Par conséquent, $n\mathbb{Z} = n'\mathbb{Z}$ donc $n\mathbb{Z} \subset n'\mathbb{Z}$ et $n'\mathbb{Z} \subset n\mathbb{Z}$.
   On en déduit que $n' \mid n$ et que $n \mid n'$ donc $n = n'$ ou $n = -n'$.
   Mais n et n' sont des entiers naturels donc $n = n'$.
   (b) **existence de** n :
   Soit H un sous groupe de $(\mathbb{Z}, +)$.
      i. **ou bien** $H = \{0\}$
      Alors $H = \{0\} = 0\mathbb{Z}$. CQFD.
      ii. **ou bien** $H \neq \{0\}$
      Alors $\exists a \in H$ avec $a \neq 0$. Par conséquent $-a \in H$. De toutes façons $\mid a \mid \in H$ avec $\mid a \mid \neq 0$.
      Soit l'ensemble $F = H \cap \mathbb{N}$. Alors F est un sous ensemble d'entiers naturels non vide donc F admet un plus petit élément n.
      Nous allons maintenant démontrer que $H = n\mathbb{Z}$
      - $n\mathbb{Z} \subset H$?
        soit $x \in n\mathbb{Z}$ donc $\exists k \in Z$ tel que $x = nk$
        donc $\mid x \mid = n \mid k \mid = n + n + \cdots + n$ (ceci $\mid k \mid$ fois).
        Or $n \in H$ et H est un sous groupe additif donc $\mid x \mid \in H$. Par conséquent, $x \in H$. CQFD.
      - $H \subset n\mathbb{Z}$?
        Soit $x \in H$. Comme $n \in \mathbb{N}^*$ alors d'après la division euclidienne $\exists!(q, r) \in (\mathbb{Z} \times \mathbb{N})$ tel que $x = nq + r$ et $0 \leq r < n$
        Alors
        — supposons que $0 < r < n$.
        Or $r = x - nq$ où $x \in H$ et $nq \in n\mathbb{Z}$.
        Or $n\mathbb{Z} \subset H$ donc $nq \in H$.
        Comme H est un sous groupe additif et que $x \in H$ et $nq \in H$ alors $x - nq \in H$.
        Par conséquent, $r \in H$.
        Donc $H \cap \mathbb{N}^*$ aurait comme plus petit élément r et non n.
        Ceci n'est pas possible.
        — donc forcément $r = 0$
        Donc $x = nq$ donc $x \in n\mathbb{Z}$. CQFD.

1.5.14 Sous groupes de $(\mathbb{R}, +)$

> ♡ ♡ ♡ Les sous-groupes additifs de $(\mathbb{R}, +)$ sont :
> 1. soit de la forme $a\mathbb{Z}$ où $a = inf(G \cap]0; +\infty[) > 0$
> 2. soit les parties denses de $\mathbb{R}$

Démonstration :
Soit G un sous groupe additif de $\mathbb{R}$. Soit $a = inf(G \cap]0; +\infty[)$

1. ou bien $a > 0$.
   Supposons que $a \notin G$:
   - Comme $2a > a$ alors $\exists x \in G$ tel que $a \leq x < 2a$ sinon $2a$ serait un minorant de G plus grand que a. Ceci est impossible car c'est a le plus grand des minorants de G.
   - Or $a \notin G$ donc $a < x < 2a$
   - De même, $\exists y \in G$ tel que $a < y < x$ sinon ce serait x qui serait le plus grand des minorants de G et non a.
   - $$\begin{cases} a < x < 2a \\ a < y < x \end{cases}$$
     donc
     $$\begin{cases} a < x < 2a \\ -x < y < -a \end{cases}$$
     d'où $a - x < x - y < a$. Or $y < x$ donc $0 < x - y$. Par conséquent, $0 < x - y < a$
   - Comme G est un groupe et que $x \in G$ et que $y \in G$ alors $x - y \in G$ avec $0 < x - y < a$. Donc $x - y$ serait le plus grand des minorants de G et non a.Ce n'est pas possible.

   Par conséquent, $a \in G$ donc $a\mathbb{Z} \subset G$.
   On peut maintenant démontrer que $G \subset a\mathbb{Z}$:
   Soit $x \in G$ alors on peut placer x entre deux multiples de a donc $\exists k \in \mathbb{Z}$ tel que $ka \leq x < (k+1)a$ donc $0 \leq x - ka < a$. Donc $x - ka$ est un élément de G plus petit que a donc forcément $x - ka = 0$ donc $x = ka$ donc $x \in a\mathbb{Z}$.
   Comme $a\mathbb{Z} \subset G$ et $G \subset a\mathbb{Z}$ alors $G = a\mathbb{Z}$. CQFD.
2. ou bien $a = 0$:
   Soit un intervalle quelconque $]\alpha; \beta[$ de réels avec $\alpha < \beta$.
   Donc $0 < \beta - \alpha$ alors $\exists x \in G$ tel que $0 \leq x < \beta - \alpha$.
   Du fait que la distance qui les sépare, deux multiples consécutifs de x ne peuvent appartenir l'un à $]-\infty; \alpha]$ et l'autre à $[\beta; +\infty[$.
   Donc $\exists k \in \mathbb{Z}$ tel que $\alpha < kx < \beta$. Par conséquent, l'intervalle $]\alpha; \beta[$ de réels contient au moins un élément de G.
   On a ainsi démontré que G est dense dans $\mathbb{R}$

1.6 Homorphismes de groupes

1.6.1 Définition

On appelle homorphisme d'un ensemble muni G d'une loi interne $\star$ dans un ensemble G' muni d'une loi interne $\perp$ toute application f de G dans G' telle que

$$\forall (x,y) \in G^2 \qquad f(x \star y) = f(x) \perp f(y)$$

.

- Tout homomorphisme bijectif de $(G,\star)$ dans $(G',\perp)$ s'appelle un isomorphisme.
- Tout homomorphisme de $(G,\star)$ dans $(G,\star)$ s'appelle un endomorphisme.
- Tout homomorphisme bijectif de $(G,\star)$ dans $(G,\star)$ s'appelle un automorphisme.

1.6.2 Exemples

1. L'application ln est un homorphisme bijectif donc un isomorphisme du groupe $(\mathbb{R}^{+*},\times)$ sur le groupe $(\mathbb{R},+)$ car :
   $\forall x > 0 \quad \forall y > 0 \quad ln(xy) = ln(x) + ln(y)$
2. L'application exp est un homorphisme bijectif donc un isomorphisme du groupe $(\mathbb{R},+)$ sur le groupe $(\mathbb{R}^{+*}$ car :
   $\forall x \in \mathbb{R} \quad \forall y \in \mathbb{R} \quad exp(x+y) = exp(x)\ exp(y)$
3. L'application
   $$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & f(x) = ax \end{array}$$
   est un automorphisme du groupe $(\mathbb{R},+)$
4. Tous les groupes à 1 élément sont isomorphes.
5. Tous les groupes à 2 éléments sont isomorphes.
6. Tous les groupes à 3 éléments sont isomorphes.
7. Si $E = \{a;b\}$ alors $\mathcal{P}(E)$ muni de la différence symétrique Δ est un groupe isomorphe au deuxième modèle de groupe d'ordre 4 : le groupe de KLEIN.

1.6.3 Propriétés

Théorème

1. Si f est un homomorphisme du groupe $(G,\star)$ dans le groupe $(G',\perp)$
   Si g est un homomorphisme du groupe $(G',\perp)$ dans le groupe $(G",\otimes)$
   Alors $g \circ f$ est un homomorphisme du groupe $(G,\star)$ dans le groupe $(G",\otimes)$
2. Si f est un isomorphisme du groupe $(G,\star)$ dans le groupe $(G',\perp)$
   Alors f^{-1} est un isomorphisme du groupe $(G',\perp)$ dans le groupe $(G,\star)$

Théorème

Si f est un homomorphisme du groupe $(G, \star)$ dans le groupe $(G', \perp)$
Si G et G' ont pour éléments neutres respectifs e et e'
Si tout élément x a pour symétrique x^{-1} dans G alors

1. $f(e) = e'$
2. $f(x^{-1}) = (f(x))^{-1}$ le symétrique de $f(x)$ dans G'
3. Le noyau de f noté $ker(f) = \{x \in G / f(x) = e'\} = f^{-1} < \{e'\} >$ est un sous-groupe de $(G, \star)$
4. L'ensemble image de G par f noté $Im(f) = f < G >= \{f(x)/x \in G\}$ est un sous-groupe de $(G', \perp)$.
5. L'image réciproque d'un sous-groupe de G' est un sous-groupe de G.

Démonstration :

1. $f(e)Tf(e) = f(e \star e) = f(e) = f(e)Te'$ donc par régularité de $f(e)$ dans le groupe (G', T) on obtient $f(e) = e'$
2. $\begin{cases} f(x)Tf(x^{-1}) = f(x \star x^{-1}) = f(e) = e' \\ f(x^{-1})Tf(x) == f(x^{-1} \star x) = f(e) = e' \end{cases}$ Par conséquent, à cause de l'unicité du symétrique d'un élément dans le groupe (G', T) ona $f(x^{-1})$ qui est le symétrique de $f(x)$ dans G'
3. On démontre aisément que le noyau de f noté $ker(f) = \{x \in G / f(x) = e'\}$ est un sous-groupe de $(G, \star)$
4. On démontre aisément que l'ensemble image de G par $f = Im(f) = f < G >= \{f(x)/x \in G\}$ est un sous-groupe de $(G', \perp)$.
5. On démontre aisément que l'image réciproque d'un sous-groupe de G' est un sous-groupe de G

Théorème

Si f est un homorphisme du groupe $(G, \star)$ dans un ensemble $(G', \perp)$
Si G et G' ont pour éléments neutres respectifs e et e'
alors

1. Le noyau de f noté $ker(f) = \{x \in G / f(x) = e'\}$ est un sous-groupe de $(G, \star)$
2. L'ensemble image de G par $f = Im(f) = f < G >= \{f(x)/x \in G\}$ est un groupe. Si de plus, f est surjective alors $(G', \perp)$ est un groupe.

Théorème

♡ ♡ ♡
Si f est un homorphisme du groupe $(G, *)$ dans un ensemble $(G', \perp)$
alors

1. f est injective $\iff ker(f) = \{e\}$
2. f est surjective $\iff Im(f) = G'$

Théorème

Si f est un isomorphisme du groupe $(G, *)$ dans un ensemble $(G', \perp)$ alors $(G', \perp)$ est un groupe.

Remarque

Prouver qu'il y a un isomorphisme entre G et un groupe "connu" est la 3ème méthode pour prouver que G est un groupe.

1.7 Automorphismes d'un groupe

1.7.1 Définition

On appelle automorphisme d'un groupe G tout homomorphisme bijectif de ce groupe dans lui-même

1.7.2 Propriétés

L'ensemble A des isomorphismes de G est un sous-groupe du groupe $\mathfrak{S}_G$ des permutations de G.

Démonstration

- $A \subset \mathfrak{S}$
- $Id_G \in A$
- Si $f \in A$ et si $g \in A$ alors $g \circ f \in A$ car la composée de deux homomorphismes est un homomorphisme et la composée de deux bijections est une bijection.
- Si $f \in A$ alors $f^{-1} \in A$ car la réciproque d'un homomorphisme bijectif est encore un homomorphisme bijectif.

1.7.3 Automorphismes intérieurs

Soit $Aut(G)$ l'ensemble des automorphismes d'un groupe G. Soit $a \in G$.

1. L'application
$$\begin{array}{rccc} \phi_a : & G & \longrightarrow & G \\ & g & \longmapsto & \phi_a(g) = aga^{-1} \end{array}$$
est un automorphisme de G appelé **automorphisme intérieur** de G.
2. L'ensemble $Int(G)$ des automorphismes intérieurs de G est un sous-groupe de A.
3. L'application
$$\begin{array}{rccc} \phi & G & \longrightarrow & Aut(G) \\ & a & \longmapsto & \phi(a) = \phi_a \end{array}$$
est un homomorphisme de G dans $Aut(G)$ dont le noyau est le centre $Z(G)$ de G. On en déduit que le groupe quotient $G/Z(G) \approx Int(G)$

Démonstration

1. (a) En notant e l'élément neutre de G, soient $(a, g, g') \in G^3$ alors $\phi_a(gg') = a(gg')a^{-1} = agg'a^{-1} = ageg'a^{-1} = (aga^{-1})(ag'a^{-1}) = \phi_a(g)\phi_a(g')$ donc ϕ_a est un homomorphisme de G dans G.
   (b) Soient $(a, a, g) \in G^3$ alors $(\phi_a \circ \phi_b)(g) = \phi_a(\phi_b(g)) = a(\phi_b(g))a^{-1} = a(bgb^{-1})b^{-1} = (ab)g(ab)^{-1} = \phi_{ab}(g)$ donc $\phi_a \circ \phi_b = \phi_{ab}$.
   Par conséquent, $\phi(ab) = \phi(a) \circ \phi(b)$ donc ϕ est un homomorphisme de G dans $Aut(G)$
   (c) En notant e l'élément neutre de G on a donc $\phi_a \circ \phi_{a^{-1}} = \phi_{aa^{-1}} = \phi_e = Id_G$. De même, $\phi_{a^{-1}} \circ \phi_a = \phi_{a^{-1}a} = \phi_e = Id_G$;
   par conséquent, $\phi_a \circ \phi_{a^{-1}} = \phi_{a^{-1}} \circ \phi_a = Id_g$ donc ϕ_a est bijective.
   (d) D'après a) et c) ϕ_a est un homomorphisme bijectif de G dans G.
2. $a \in Ker(\phi) \iff \phi(a) = Id_G \iff \phi_a = Id_G \iff \forall g \in G \phi_a(g) = Id_G(g) \iff aga^1 = g \iff ag = ga \iff a \in Z(G)$

1.7.4 Propriété

Le seul automorphisme intérieur d'un groupe commutatif G est Id_G

1.8 Sous-groupes distingués

1.8.1 Définition

Soit $(G, .)$ un groupe. Soit H un sous-groupe de G.
Les 3 propositions suivantes sont équivalentes :

- (i) : $\forall x \in G \quad xHx^{-1} \subset H$
- (ii) : $\forall x \in G \quad xHx^{-1} = H$
- (iii) : $\forall x \in G \quad xH = Hx$

Si l'une de ces 3 conditions est vérifiée, on dit que H est un sous-groupe distingué de G. On note alors $H \lhd G$

Démonstration

1. Il est évident que $(iii) \iff (ii)$
2. Il est évident que $(ii) \implies (i)$
3. Reste seulement à prouver que $(i) \implies (ii)$ en prouvant que $H \subset xHx^{-1}$
   Soit $x \in G$ alors $H = eHe = (x^{-1}x)H(x^{-1}x) = x^{-1}(xHx^{-1})x \subset x^{-1}Hx$ car $xHx^{-1} \subset H$

1.8.2 Propriétés

1. Tous les sous-groupes d'un groupe commutatif G sont forcément distingués.
2. Les sous-groupes triviaux G et $\{e\}$ sont distingués dans G.
3. Le centre d'un groupe G à savoir $Z(G) = \{x \in G \ / \ \forall g \in G \quad xg = gx\}$ est distingué dans G.
4. Le noyau $ker(f)$ d'un homomorphisme d'un groupe G dans un groupe G' est distingué dans G.
5. Si H est un sous-groupe distingué de G et si f est un morphisme surjectif du groupe $(G, .)$ sur le groupe $(G', .)$ alors $f(H)$ est un sous-groupe distingué de G'.

1.8.3 Démonstration

1. évident.
2. - $\{e\}$ est distingué car $\forall x \in G \quad xex^{-1} = (xe)x^{-1} = xx^{-1} = e \in \{e\}$
   - G est distingué car $\forall x \in G \quad \forall g \in G \quad xgx^{-1} \in G$ car le produit de 3 éléments d'un groupe est un élément de ce même groupe.
3. Soit $x \in G$. Soit $c \in Z(G)$. Soit $y \in G$
   alors $[xcx^{-1}]y = (xc)x^{-1}y = (cx)x^{-1}y$ car $cx = xc$ puisque $c \in Z(G)$.
   Donc $[xcx^{-1}]y = c(xx^{-1})y = (ce)y = cy = yc$ puisque $c \in Z(G)$.
   $[xcx^{-1}]y = yc = yce = yc(xx^{-1}) = y(cx)x^{-1}) = y(xc)x^{-1} = y[xcx^{-1}]$
   donc $xcx^{-1} \in Z(G)$.
4. Soit $x \in G$. Soit $k \in Ker(f)$.
   Alors $f(xkx^{-1}) = f(x)f(k)f(x^{-1}) = f(x)f(k)[f(x)]^{-1}$ car f est un morphisme de groupe.

Or $k \in ker(f)$donc $f(x) = 0_{G'}$.
Par conséquent, $f(xkx^{-1} = f(x)0_{G'}[f(x)]^{-1} = 0_{G'}$ donc $xkx^{-1} \in ker(f)$.
CQFD.

5. Soit f un morphisme surjectif de G dans G'. Soit H un sous-groupe distingué de G
   - $f(H)$ est un sous-groupe de G' car
     — $f(H) \subset G'$
     — $f(H) \neq \emptyset$ car l'élément neutre e' de G' appartient à $f(H)$ puisque f étant un morphisme, l'on sait que $e' = f(e)$ avec $e \in H$.
     — Si $y_1 \in f(H)$ et $y_2 \in f(H)$ alors $\exists x_1 \in H$ et $\exists x_2 \in H$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$.
     Alors $y_1 y_2^{-1} = f(x_1)[f(x_2)]^{-1} = f(x_1)f(x_2^{-1}) = f(x_1 x_2^{-1})$ car f est un morphisme.
     Or H est un sous groupe,
     comme $x_1 \in H$ et $x_2 \in H$ alors $x_1 x_2^{-1} \in H$.
     Donc $y_1 y_2^{-1} = f(x_1 x_2^{-1} \in f(H)$.
   - Il reste à prouver que $f(H)$ est distingué dans G'.
     Pour cela , prouvons que $\forall y \in G' \quad yf(H)y^{-1} \in f(H)$.
     Soit $z \in yf(H)y^{-1}$ donc $\exists h \in H \quad z = yf(h)y^{-1} = f(x)f(h)[f(x)]^{-1}$ car f étant surjective il existera $x \in G$ tel que $y = f(x)$.
     Par conséquent, $z = f(x)f(h)f(x)^{-1}) = f(xhx^{-1})$ puisque f est un morphisme.
     Or $x \in G$ et H est distingué dans G donc $xhx^{-1} \in H$ donc $z \in f(H)$.
     CQFD.

1.8.4 Sous groupe distingué et automorphisme intérieur

Soit G un groupe et H un sous-groupe de G. Alors
$H \lhd G \iff \forall x \in G \quad xHx^{-1} = H \iff \forall x \in G \quad \alpha_x(H) = H$
$\iff$ H est invariant par tout automorphisme intérieur.

1.9 Exercices

1.9.1 Exercice

> Dans un groupe multiplicatif G , si chaque élément est son propre symétrique alors ce groupe G est commutatif.

Corrigé

Il suffira de démontrer que yx est le symétrique de xy.

1. Soit $(x, y) \in G^2$ alors $xy \in G$
2. Comme chaque élément est son propre symétrique :
   $(xy)(yx) = xyyx = xyy^{-1}x = xex = xx = xx^{-1} = e$
3. Donc $yx = (xy)^{-1}$.
   Or chaque élément est son propre symétrique donc $yx = xy$ CQFD.

1.9.2 Exercice

> Soit un ensemble E. Soit f une application involutive de E dans E (c'est-à-dire telle que $f \circ f = Id_E$.
> Démontrer que $H = \{Id_E, f\}$ est un sous-groupe du groupe des transformations $\mathcal{J}(E)$.

Corrigé

Comme $f \circ f = Id_E$ alors f est bijective et $f^{-1} = f$ d'où la table de H :

$\circ$	Id_E	f
Id_E	Id_E	f
f	f	Id_E

H est bien un sous-groupe du groupe $\mathcal{J}(E)$ car

1. la composée de deux éléments de H est encore un élément de H
2. tout élément de H admet un symétrique (lui-même) dans H

1.9.3 Exercice

Soit $(G, \star)$ un groupe d'élément neutre e. Soit $a \in G$. Soit une loi interne T définie sur G par $xTy = x \star a \star y$.
Démontrer que (G, T) est un groupe.

Corrigé

1. T est interne par définition.
2. T est associative car :
   $\forall (x, y, z) \in G^3 \quad xT(yTz) = x \star a \star (yTz) = x \star a \star (y \star a \star z)$.
   Or $\star$ est associative donc on peut déplacer la parenthèse :
   $xT(yTz) = (x \star a \star y) \star a \star z = (xTy) \star a \star z = (xTy)Tz$
3. T admet pour élément neutre a^{-1} car :
   $\forall x \in G \left\{ \; xTa^{-1} = x \star a \star a^{-1} = x \star e = xa^{-1}Tx = a^{-1} \star a \star x = e \star x = x \right.$
4. Tout élément x de G admet un symétrique pour T c'est $a^{-1} \star x^{-1} \star a^{-1}$ car :
   $\forall x \in G \left\{ \; xT(a^{-1} \star x^{-1} \star a^{-1}) = x \star \star a \star a^{-1} \star x^{-1} \star a^{-1} = a^{-1}(a^{-1} \star x^{-1} \star a^{-1})Tx = a^{-1} \star x^{-1} \star a^{-1} \star a \star x = a \right.$

. En conclusion, (G, T) est un groupe.

1.9.4

Soit un groupe multiplicatif $(G, .)$. Démontrer que si $f : x \mapsto x^{-1}$ est un morphisme alors le groupe G est commutatif.

Corrigé

Soient $x \in G$ et $y \in G$. Comme f est un morphisme alors $f(xy) = f(x)f(y)$ donc $(xy)^{-1} = x^{-1}y^{-1}$.
On a alors $y^{-1}x^{-1} = x^{-1}y^{-1}$. Ce qui implique que $xyy^{-1}x^{-1} = xyx^{-1}y^{-1}$.
On a donc $xx^{-1} = xyx^{-1}y^{-1}$. On obtient donc $1 = xyx^{-1}y^{-1}$ d'où $yx = xyx^{-1}y^{-1}yx$ donc $yx = xyx^{-1}x$ d'où $yx = xy$. CQFD.

1.9.5

Soit un groupe multiplicatif $(G, .)$. Soit $a \in G$.
Démontrer que l'application

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & G \\ & \bar{n} & \longmapsto & f(\bar{n}) = a^n \end{array}$$

est un homomorphisme du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ dans le groupe $(G, .)$

Corrigé

1.9.6 Une condition minimale pour avoir un groupe

Soit E muni d'une loi associative notée multiplicativement.
On suppose qu'il existe un élément neutre à gauche noté e_g et que tout élément de E admet un inverse à gauche pour le neutre à gauche
(c'est-à-dire $\forall x \in E \quad \exists x'_g \in E \quad x'_g.x = e_g$)

1. Démontrer que $x.x'_g = e_g$.
2. Démontrer que e_g est aussi neutre à droite.
3. En déduire que E est un groupe.

1.9.7 Produit de deux sous-groupes

1. Soient H et K deux sous-groupes d'un même groupe $(G, .)$ d'élément neutre e.
   On rappelle que $H.K = \{x.y/(x, y) \in H \times K\}$
   Montrer que :
   $H.K$ est un sous-groupe de G si et seulement si $H.K = K.H$
   Attention ! Cela ne veut pas dire que $\forall h \in H \quad \forall k \in K \quad hk = kh$
2. On suppose que H et K sont deux sous-groupes finis du groupe $G, .)$et que $H \cap K = \{e\}$
   Démontrer que :
   $H.K$ est fini et que $card(H.K) = card(H).card(K)$

Chapitre 2

Groupes opérant sur un ensemble

2.1 Définition

Soit un groupe G d'élément neutre e et un ensemble X.
On dira que G opère sur X lorsqu'il existera une application :

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g,x) & \mapsto & g.x \end{array}$$

telle que

1. $\forall (g,g') \in G^2 \quad \forall x \in X \quad g.(g'.x) = (gg').x$
2. $\forall x \in X \quad e.x = x$

2.1.1 Remarque

En appelant S_X l'ensemble des permutations de l'ensemble X, il reviendrait de même de construire un morphisme

$$\phi : \begin{array}{ccc} G & \longrightarrow & S_X \\ g & \mapsto & \phi(g) \end{array}$$

tel que $\phi(g)(x) = g.x$

2.2 Exemples

1. $G = S_X$ opère sur X en prenant pour morphisme $\phi = Id_{S_X}$
2. Si $H < G$ alors H opère sur G par translation à gauche

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h,g) & \mapsto & h.g = hg \end{array}$$

3. Si $H < G$ alors H opère sur G par automorphisme intérieur

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h,g) & \mapsto & h.g = hgh^{-1} \end{array}$$

4. $GL_n(\mathbb{R})$ opère sur $\mathbb{R}^n$
5. S^1 opère sur $\mathbb{C}$ par exponentation complexe(à vérifier)

2.3 Définition

G opère transitivement sur X si $\forall (x,y) \in X^2 \quad \exists g \in G \quad g.x = y$

2.3.1 Exemples

$GL_n(\mathbb{R})$ n'opère pas transitivement sur $\mathbb{R}^n$ mais sur $\mathbb{R}^n - \{0\}$

2.4 Orbites

Soit G opérant sur X.
Soit la relation $\mathcal{R}$ définie sur X par

$$x\mathcal{R}y \iff \exists g \in G \quad y = g.x$$

Alors $\mathcal{R}$ est une relation d'équivalence sur G et les classes d'équivalence qui sont de la forme Gx sont appelées **orbites ou trajectoires**.

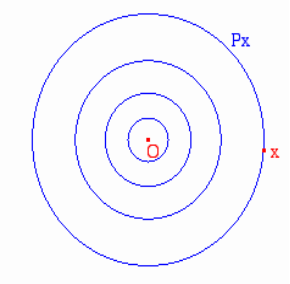
2.4.1 2 orbites particulières

Orbite 1

Soit un point O du plan affine euclidien P et soit G le groupe des rotations de centre O muni de la loi de composition o des applications.
Alors G opère sur P par

$$\begin{array}{ccc} G \times P & \longrightarrow & P \\ (r, M) & \mapsto & r.M = r(M) \end{array}$$

Les orbites sont alors les cercles concentriques de centre O.

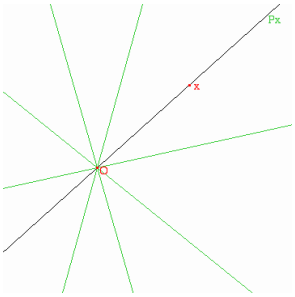


Orbite 2

Soit un point O du plan affine euclidien P et soit G le groupe des homothéties de centre O muni de la loi de composition o des applications.
Alors G opère sur P par

$$\begin{array}{ccc} G \times P & \longrightarrow & P \\ (h, M) & \mapsto & h.M = h(M) \end{array}$$

Les orbites sont alors les droites passant par O.



2.5 Stabilisateur

2.5.1 Définition

Pour tout $x \in X$ l'ensemble $S(x) = \{g \in G / g.x = x\}$ est un sous-groupe de G
appelé stabilisateur de x

2.5.2 Première formule de dénombrement

Si G est un groupe fini et si $G.x$ désigne l'orbite de x alors $Card(G) = Card(G.x) \times Card(S(x))$

Démonstration 1

Soit $y \in G.x$. Soit $C_y = \{g \in G / y = g.x\}$.
Si h est un élément particulier de C_y alors on peut définir la bijection

$$\begin{array}{ccc} C_y & \longrightarrow & S(x) \\ g & \longmapsto & h^{-1}g \end{array}$$

alors $Card(C_y) = Card(S(x))$
Par conséquent, $Card(G) = \sum_{y \in G.x} Card(C_y) = \sum_{y \in G.x} Card(S(x)) = Card(w(x)) \times Card(S(x))$

Démonstration 2

L'application

$$\begin{array}{ccc} \dfrac{G}{G_x} & \longrightarrow & G.x \\ \dot{g} & \longmapsto & g.x \end{array}$$

est bien définie et est bijective donc $Card(G.x) = \dfrac{Card(G)}{Card(G_x)}$

2.5.3 Théorème de Burnside-Frobenius

Si G est fini, soit Ω l'ensemble des orbites.
Pour tout élément $g \in G$ on pose $A_g = \{x \in E / g.x = x\}$
Alors

$$Card(\Omega) = \frac{1}{Card(G)} \sum_{g \in G} Card(A_g)$$

Démonstration

Soit $U = \{(g, x) \in G \times E / g.x = x\}$ alors
$Card(U) = \sum_{g \in G} Card(A_g) = \sum_{g \in G} \sum_{x \in E} Card(S(x))$
$= \sum_{g \in G} \sum_{x \in \omega} \frac{Card(G)}{Card(\omega)} = \sum_{\omega \in \Omega} Card(G) = Card(\Omega) \times Card(G)$

2.6 Applications

2.6.1 Algèbre

Lemme

Si G est un groupe fini qui opère sur lui-même par conjugaison alos

$$Card(G) = Card(Z(G)) + \sum_i [G : G_{x_i}]$$

Applications

1. Le centre $Z(G)$ de tout $p-$groupe n'est pas vide.
2. Si $Card(G) = p^2$ où p est 1^{er} alors$G$ est abélien

Théorème de Sylow

Si G est un groupe fini et p un diviseur premier de l'ordre n de G alors G contient un $p-$sous groupe de Sylow

Théorème

Lorsque S_n opère sur lui-même par conjugaison alors les trajectoires sont les cycles de même type.

Théorème

Les $3-$cycles sont conjugués dans $\mathcal{A}_n$ pour $n \geq 5$.

Application

$\mathcal{A}_5$ est simple.

2.6.2 Géométrie

Théorème

$\mathcal{O}(\mathbb{R})$ et $\mathcal{O}^+(\mathbb{R}^n)$ opèrent transitivement sur l'espace euclidien $\mathbb{R}^n$

$$\mathcal{S}^{n-1} \simeq \frac{\mathcal{O}(\mathbb{R}^n)}{\mathcal{O}(\mathbb{R}^n)_x} \simeq \frac{\mathcal{O}(\mathbb{R}^n)}{\mathcal{O}(\mathbb{R}^{n-1})}$$

Théorème

Soit G un sous groupe fini de $\mathcal{O}^+(\mathbb{R}^3)$ et d'ordre $n > 1$.
Soit $P = \{\text{pôles de } g \in G - \{ e\}\}$ Alors

1. G opère dans P
2. G_x est cyclique et $2 \leq Card(G_x) \leq n$
3. $n\sum_{x_i}(1 - Card(G_{x_i}) = 2(n-1)$.

   Ceci permet de dénombrer le nombre de sous groupes finis de $\mathcal{O}^+(\mathbb{R}^3)$

Chapitre 3

Groupes monogènes

3.1 Définitions et propriétés

3.1.1 Définition

Soit $(G, .)$ un groupe d'élément neutre e. Soit $a \in G$. Alors l'ensemble suivant $< a >= \{a^\lambda / \lambda \in \mathbb{Z}\}$ est un sous-groupe de G appelé le sous-groupe engendré par a ou encore le groupe monogène engendré par a.
L'ordre de ce sous-groupe $< a >$ c'est-à-dire son cardinal est appelé aussi l'ordre de l'élément a.
L'ordre d'un élément a est le plus petit entier $k \in \mathbb{N} \quad a^k = e$

3.1.2 Propriété

Si l'on note a^{-1} l'élément symétrique de a dans G alors $< a >=< a^{-1} >$

3.1.3 Exemples d'ordres d'éléments

- Soit $\tau = (i, j)$ une transposition c'est-à-dire un 2-cycle dans S_n alors $ordre(\tau) = 2$ car $\tau^2 = \tau \circ \tau = (i, j)(i, j) = id$
- L'ordre d'un $3-$cycle (a, b, c) dans S_n est 3 car $(a, b, c)^3 = (a, b, c)(a, b, c)(a, b, c) = id$
- L'ordre de la permutaion $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$ est 6
  car $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$
  $\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} \qquad \sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}$
  $\sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \qquad \sigma^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = id$

3.1.4 Définition d'un groupe monogène

Un groupe G est dit monogène s'il coïncide avec l'un de ses sous-groupes monogènes, c'est-à-dire $\exists\ a \in G$ tel que $G =< a >$

3.1.5 Propriété

Si le groupe G est monogène avec $G =< a >$

- ou bien l'application $\lambda \mapsto a^{\lambda}$ est injective
  Alors a est dit d'ordre infini et G est dit **monogène infini**.
  Exemple : $\mathbb{Z} =< 1 >=< -1 >$
- ou bien l'application $\lambda \mapsto a^{\lambda}$ n'est pas injective
  Alors $\exists\ k \in \mathbb{Z}\ a^k = e$.
  Soit n le plus petit de ces k, alors $G =< a >= \{e, a, a^2, a^3, ..., a^{n-1}\}$
  G est monogène fini.
  On dit alors que c'est un **groupe cyclique d'ordre n**.

3.1.6 Isomorphisme de 2 groupes monogènes infinis

2 groupes monogènes infinis $< a >$ et $< b >$ sont isomorphes par l'application : $a^\lambda \mapsto b^\lambda$

3.1.7 Isomorphisme d'un groupe cyclique d'ordre n et de $\frac{\mathbb{Z}}{n\mathbb{Z}}$

- Si G est un groupe monogène infini alors $G \approx (\mathbb{Z}, +)$
- Si G est un groupe cyclique d'ordre n alors $G \approx \frac{\mathbb{Z}}{n\mathbb{Z}}$

Démonstration

L'application ϕ de $\mathbb{Z}$ dans $G : n \mapsto a^n$ est un homomorphisme de groupes.
En effet, soit $(n, p) \in \mathbb{Z}^2$ alors $\phi(n+p) = a^{n+p} = a^n a^p = \phi(n)\phi(p)$.
Par conséquent, $G \approx \dfrac{\mathbb{Z}}{ker\phi}$
ou bien $ker(\phi) = \{0\}$ alors $G \approx \mathbb{Z}$
ou bien $ker(\phi) \neq \{0\}$ alors $G \approx \dfrac{\mathbb{Z}}{ker\phi}$

3.2 Propriétés des groupes cycliques

3.2.1 Théorème

Tout sous-groupe d'un groupe cyclique est cyclique.

démonstration

Soit G un groupe cyclique $< a >$ et H un de ses sous-groupes.
Comme l'application ϕ de $\mathbb{Z}$ dans $G : n \mapsto a^n$ est un homomorphisme de groupe, alors $\phi^{-1} < H >$ est un sous-groupe de $\mathbb{Z}$ donc est de la forme $r\mathbb{Z}$.
Alors $H = \phi < \phi^{-1} < H >>= \{a^{rk}/k \in \mathbb{Z}\} =< a^r >$ donc H est cyclique.
CQFD.

3.2.2 Théorème

L'image par un homomorphisme d'un groupe cyclique est un groupe cyclique.

démonstration

Soit un groupe cyclique $G =< a >$. Soit ϕ un homomorphisme défini sur G.

- Soit $y \in \phi(G)$.
  Alors $\exists x \in G \quad y = \phi(x)$.
  Or $\exists n \in \mathbb{N}\ x = a^n$. Donc $y = \phi(a^n) = \phi(a)^n$ d'où $y \in < \phi(a) >$
  Par conséquent, $\phi(G) \subset < \phi(a) >$.
- Or $< \phi(a) > \subset \phi(G)$
- donc $\phi(G) =< \phi(a) >$

Par conséquent $\phi(G)$ est cyclique.CQFD

3.2.3 Sous groupes de $\mathbb{Z}$

Les seuls sous-groupes du groupe additif $\mathbb{Z}$ sont les $a\mathbb{Z}$ qui sont isomorphes à $\mathbb{Z}$.

démonstration

$\mathbb{Z}$ est cyclique engendré par 1 et donc tous ses sous-groupes sont cycliques.
Soit G un sous-groupe de $\mathbb{Z}$ alors $G =< a >$ donc $G = a\mathbb{Z}$ où a est le plus petit élément positif de G.
L'application $\phi : n \mapsto an$ est un isomorphisme du groupe additif $\mathbb{Z}$ dans le groupe additif $a\mathbb{Z}$

3.2.4 Théorème

Si G_1 et G_2 sont des sous-groupes alors $(G_1 \cup G_2) = G_1 + G_2$.
Par conséquent, $(a\mathbb{Z} \cup b\mathbb{Z}) = a\mathbb{Z} + b\mathbb{Z}$

démonstration

- Démontrons d'abord que $G_1 + G_2 \subset (G_1 \cup G_2)$.
  Soit $a \in G_1 + G_2$ donc $a = g_1 + g_2$ où $g_1 \in G_1$ et $g_2 \in G_2$.
  On sait que $G_1 \subset G_1 \cup G_2$ donc $G_1 \subset (G_1 \cup G_2)$.
  Or $g_1 \in G_1$ et $G_1 \subset (G_1 \cup G_2)$ donc $g_1 \in (G_1 \cup G_2)$.
  De même, $g_2 \in (G_1 \cup G_2)$.
  Donc $a = g_1 + g_2 \in (G_1 \cup G_2)$
- Démontrons ensuite que $(G_1 \cup G_2) \subset G_1 + G_2$.

  — Tout d'abord $G_1 + G_2$ est un groupe : en effet, soit $a \in G_1 + G_2$, soit $b \in G_1 + G_2$ alors $a = g_1 + g_2$ et $b = g'_1 + g'_2$ où $g_1, g'_2 \in G_1$ et $g_2, g'_2 \in G_2$.
  Par conséquent $a - b = (g_1 + g_2) - (g'_1 + g'_2) = (g_1 - g'_1) + (g_2 - g'_2) \in G_1 + G_2$ car $(g_1 - g'_1) \in G_1$ puisque G_1 est un groupe et $(g_2 - g'_2) \in G_2$ puisque G_2 est un groupe
  — $G_1 \cup G_2 \subset G_1 + G_2$ car $G_1 \subset G_1 + G_2$ et $G_2 \subset G_1 + G_2$
  — $G_1 + G_2$ est donc un groupe contenant $G_1 \cup G_2$ donc $(G_1 \cup G_2) \subset G_1 + G_2$

3.2.5 Théorème

$a\mathbb{Z} \cap b\mathbb{Z} = (ppcm(a, b))\mathbb{Z}$

démonstration

- $a\mathbb{Z}$ et $b\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$ donc $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$. Or les sous groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ donc $\exists c \in \mathbb{Z}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$
- Comme $a\mathbb{Z} \cap b\mathbb{Z} = c\mathbb{Z}$ alors $c\mathbb{Z} \subset a\mathbb{Z}$ donc $a \mid c$
- De même $b \mid c$
- Soit k un multiple commun à a et à b donc $a \mid k$ et $b \mid k$ donc $k\mathbb{Z} \subset a\mathbb{Z}$ et $k\mathbb{Z} \subset b\mathbb{Z}$ d'où $k\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$ donc $k\mathbb{Z} \subset c\mathbb{Z}$ donc $c \mid k$
- Par conséquent k est le plus petit commun multiple de a et de b. CQFD.

3.2.6 Théorème

> $a\mathbb{Z} + b\mathbb{Z} = (pgcd(a,b))\mathbb{Z}$

démonstration

- $a\mathbb{Z} + b\mathbb{Z} = (a\mathbb{Z} \cup b\mathbb{Z})$ donc $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ donc $\exists k \in \mathbb{Z}$ tel que $a\mathbb{Z} + b\mathbb{Z} = k\mathbb{Z}$
- $a\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$ donc $a\mathbb{Z} \subset k\mathbb{Z}$ donc $k \mid a$
- De même $k \mid b$
- Soit $q \mid a$ et $q \mid b$ donc $a\mathbb{Z} \subset q\mathbb{Z}$ et $b\mathbb{Z} \subset q\mathbb{Z}$ donc $a\mathbb{Z} \cup b\mathbb{Z} \subset q\mathbb{Z}$ d'où $(a\mathbb{Z} \cup b\mathbb{Z}) \subset q\mathbb{Z}$. Par conséquent $a\mathbb{Z} + b\mathbb{Z} \subset q\mathbb{Z}$ donc $k\mathbb{Z} \subset q\mathbb{Z}$. On en déduit que $q \mid k$
- Par conséquent, k est le plus grand commun diviseur à a et à b

3.2.7 Théorème de Bezout

> Si $d = a \wedge b$ alors $\exists (u,v) \in \mathbb{Z}^2$ tel que $au + bv = d$

démonstration

Soit $d = a \wedge b$ alors $d = d.1 \in (pgcd(a,b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ donc $\exists (u,v) \in \mathbb{Z}^2$ tel que $d = au + bv$

3.2.8 Théorème

> 1. Tout groupe monogène infini est isomorphe à $\mathbb{Z}$
> 2. Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

Démonstration

Soit G un groupe cyclique donc $G = (g)$. Soit

$$\phi : \mathbb{Z} \mapsto G$$

$$n \mapsto \phi(n) = g^n$$

- ϕ est un homomorphisme surjectif de $\mathbb{Z}$ sur G
- L'ordre $O(G)$ de G est l'ordre de g
- ou bien $O(G) = +\infty$ donc $O(g) = +\infty$. Par conséquent, si $g^n = e$ alors $n = 0$ donc $ker(\phi) = \{0\}$ donc ϕ est injective. ϕ devient donc un isomorphisme entre $\mathbb{Z}$ et G. CQFD.
- ou bien $O(G) = n$ donc $ker(\phi) = n\mathbb{Z}$. D'après le premier théorèm d'isomorphisme, l'on a : $G \simeq \mathbb{Z}/n\mathbb{Z}$

3.2.9 Théorème

> Soit H un sous-groupe de G.
> Alors les sous-groupes de G/H sont les quotients par H des sous-groupes de G contenant H.

Démonstration

Soit

$$f : G \mapsto G/H$$
$$x \mapsto f(x) = \dot{x}$$

On sait que f est surjective et non injective.
Soit K un sous-groupe de G/H, alors $\dot{e} \in K$ donc $f^{-1}(K)$ est un sous-groupe de G contenant $f^{-1}(\dot{e}) = H$. Par conséquent $K = f(f^{-1}(K)) = f^{-1}(K)/H$.
On en déduit que les sous-groupes de G/H sont les quotients par H des sous-groupes de G contenant H

3.2.10 Corollaire

> Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques de la forme $d\mathbb{Z}/n\mathbb{Z}$ et sont au nombre de $\frac{n}{d}$.
> En particulier, $a\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/b\mathbb{Z}$.

Démonstration

Soit $d\mathbb{Z}$ un sous-groupe de $\mathbb{Z}$ contenant $n\mathbb{Z}$ donc $d \mid n$ et les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ avec $d \mid n$. Or $\mathbb{Z}/n\mathbb{Z}$ est cyclique donc $d\mathbb{Z}/n\mathbb{Z}$ est cyclique. Ordre$(d\mathbb{Z}/n\mathbb{Z})$ = ordre$(\bar{d})$ = le plus petit k tel que $dk \in n\mathbb{Z}$. C'est $k = \frac{n}{d}$ et $d\mathbb{Z} \simeq \mathbb{Z}/\frac{n}{d}\mathbb{Z}$ donc les sous -groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques de la forme $d\mathbb{Z}/n\mathbb{Z}$ et sont au nombre de $\frac{n}{d}$. En particulier, $a\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/b\mathbb{Z}$

3.3 Notion de $p-$groupe

3.3.1 Théorème

Si p est $1er$ et si p divise n l'ordre du groupe G fini commutatif alors G contient un élément d'ordre p.

Démonstration

Raisonnons par récurrence sur l'ordre $n = \mathcal{O}(G)$

1. **ou bien G n'a pas de sous-groupe propre.**
   Donc $\mathcal{O}(G)$ est premier donc G est cyclique d'ordre p et tout générateur de G est alors d'ordre p
2. **ou bien G a au moins un sous-groupe propre.**

   (a) ou bien G a un sous groupe propre H tel que $p \mid \mathcal{O}(H)$.
   D'après l'hypothèse de récurrence, comme $H < G$ alors $\mathcal{O}(H) < \mathcal{O}(G) = n$. Donc H contient un élément a d'ordre p . Or $a \in G$. Par conséquent , G contient cet élément a d'ordre p.

   (b) ou bien p ne divise pas q l'ordre de n'importe quel sous groupe H de G.

   - Or $\mathcal{O}(G) = n = pCard(G/H)$ Comme p ne divise aucun q alors comme $p \mid n$ donc $p \mid Card(G/H)$. or $O(G/H) < n$. D'après l'hypothèse de récuurence, il existe $\bar{a} \in G/H$ tel que $ordre(\bar{a}) = p$. Donc $\bar{a} = aH$ Or $\bar{a}^p = \bar{e} = H$.
   - Comme $\bar{a} \neq \bar{e}$ donc $aH \neq H$ donc $a \notin H$ Mais $\bar{a}^p = H$ donc $a^p \in H$ car $a^p H = H$. Comme $a^p \in H$ alors $(a^p)^q = e$ et $\mathcal{O}(H) = q$
   - Soit $b = a^q$. Supposons que $b = e$ alors $\bar{a}^q = (aH)^q = a^q H = bH = H = \bar{e}$.
     Donc $\bar{a}^q = \bar{e}$ donc $a \in H$. Ceci est faux. Par conséquent $b \neq e$.
     Comme $b^p = e$ et $p1^{er}$ et $b \neq e$ alors b est d'ordre p dans G.

Remarque

G a donc un sous-groupe cyclique propre d'ordre p. C'est un premier élément de réponse à la réciproque du Théorème de Lagrange.

Définition

Si p est 1^{er}, on appelle $p-$groupe tout groupe fini dont l'ordre est une puissance de p.

Chapitre 4

Les 2 théorèmes de Sylow

4.1 Théorème 1 de Sylow

4.1.1 Définition

Soit G un groupe fini d'ordre ou de cardinal n.
Soit p un diviseur premier de n donc $\exists\ \alpha \in \mathbb{N}^*\ n = p^\alpha m$ où m et p sont premiers entre eux.
On appelle $p-$ sous-groupe de Sylow de G tout sous-groupe d'ordre p^α : la plus grande puissance de p divisant l'ordre n de G.
Si S est un $p-$sous groupe de Sylow de G , soit $[G : S]$ l'indice de S dans G qui est premier avec p..

- ou bien $S \lhd G$.
  Alors $[G : S]$ est le nombre de classes d'équivalence modulo S
- ou bien on n'a pas $S \lhd G$
  Alors $[G : S]$ est le nombre de classes d'équivalence à gauche modulo S = nombre de classes d'équivalence à droite modulo S

4.1.2 Théorème

Si n est divisible par une puissance p^α oùp est 1^{er}
Alors tout groupe G fini d'ordre n contient un sous-groupe d'ordre p^α

Démonstration

On fera une démonstration par récurrence sur n.
L'hypothèse de récurrence est : " supposons que la propriété est vraie pour tout groupe d'ordre $< n$ et d'ordre divisible par p^α."
On sait que g opère sur G par conjugaison :

$$\begin{array}{ccc} G \times G & \to & G \\ (g, x) & \to & g\ x\ g^{-1} \end{array}$$

Soit $Z(G)$ le centre de G. C'est l'ensemble des éléments de G qui ne sont pas conjugués.

1. **ou bien on peut trouver $x \in G - Z(G)$ tel que $card(G_x)$ ne soit pas divisible par p.**
   On sait que $n = Card(H_x)\ Card(G_x)$. Or $p \mid Card(H_x)$. On sait que

$ordre(H_x) = Card(H_x) < ordre(G) = n$.
$p^k \mid n = card(H_x$ et p ne divise pas $Card(G_x)$ donc $p^{\cdots}$ ne divise pas $Card(G_x)$ donc $Card(H_x)$ est divisible par $p^{\cdots}$
D'après l'hypothèse de récurrence, H_x contient un sous-groupe d'ordre p^α donc G contient un sous-groupe d'ordre p^α CQFD.

2. **ou bien** $\forall x \in G - Z(G)$ **on a** $p \mid Card(G_x)$
D'après l'équation des classes, $q = card(Z(G)) = n - \sum_{x \in A} Card(G_x)$ où A est l'ensemble des ... qui contient un élément de chaque ordre.
$p \mid n$ et $\forall x \in G\ p \mid Card(G_x)$ donc $p \mid q = Card(Z(G))$.
Comme $p \mid q$ donc $Z(G)$ n'est pas trivial. $p \mid Z(G)$ qui est commutatif et p est 1^{er} donc $Z(G)$ contient un élément a d'ordre p.
Soit $H = (a)$. On a $H \lhd G$ et $p^\alpha \mid O(G)$. Or $p = O(H)$ donc $p^{\alpha-1} \mid O(G/H)$. Comme H est non trivial donc $O(G/H) < O(G)$ donc par hypothèse de récurrence G/H contient un sous-groupe K' d'ordre $p^{\alpha-1}$
On va revenir à G par l'épimorphisme $\phi : G \mapsto G/H$. Soit $K = \phi^{-1}(K')$
On a $K \subset G$. On sait que $H \subset K$ et que $\phi/K : K \mapsto K'$ est un épimorphisme qui a pour noyau H. Donc $K/H \simeq K'$ d'où $ordre(K) = ordre(H)\ ordre(H') = p\ p^{\alpha-1} = p^\alpha$ donc G contient K un sous-groupe d'ordre p^α

4.1.3 Théorème 1 de Sylow

Si G est un groupe fini de cardinal n et si p est un diviseur 1^{er} de n
Alors il existe un $p-$sous-groupe de Sylow de G.

Démonstration

Ce théorème découle du théorème précédent. $O(G = p^\alpha m$ où p et m sont premiers entre eux et $\alpha \in \mathbb{N}^*$

4.1.4 Remarque

Tout conjugué d'un $p-$sous-groupe de Sylow de G est un $p-$sous-groupe de Sylow de G

Démonstration

Si S est un $p-$sous-groupe de Sylow de G alors $O(S) = p^\alpha$. Si S' est un conjugué de S alors $\exists x \in G\ S' = xSx^{-1}$.
Alors $O(S') = O(S) = p^\alpha$ donc S' est un $p-$sous-groupe de Sylow de G

4.2 Deuxième Théorème de Sylow

4.2.1 Théorème préliminaire

Si P est un $p-$sous-groupe de Sylow de G alors tout sous-groupe du normalisateur de P est contenu dans P.

Démonstration

Soit R un $p-$sous-groupe de G contenu dans $N(P)$. On sait que $P \lhd N(P)$. Donc $R < N(P)$.
D'après le théorème 2 d'isomorphisme des groupes on a $\frac{R}{P \cap R} \simeq \frac{PR}{P}$. Comme $O(\frac{R}{P \cap R})$ est donc une puissance de p donc $\frac{PR}{P}$ a un ordre qui est une puissance de p donc $O(PR)$ est une puissance de p car P est un $p-$sous-groupe de Sylow. Donc PR est un $p-$sous-groupe de G qui contient P qui est un $p-$sous-groupe de Sylow.
Par conséquent, son ordre est la puissance maximale de p donc $PR = P$.
D'où $R \subset P$.

4.2.2 Théorème 2 de Sylow

Soit G un groupe fini d'ordre $n = p^\alpha m$ où p $1^{er}, \alpha \in \mathbb{N}^*$ et m et p premiers entre eux.
Alors

- tout $p-$sous-groupe de G est contenu dans un $p-$sous-groupe de Sylow de G
- les $p-$sous-groupes de Sylow de G sont conjugués et leur nombre est congru à 1 modulo p. Ce nombre divise n.

Démonstration

1. Soit P un $p-$sous groupe de G. Soit S un $p-$sous groupe de Sylow de G.
   Alors $O(G) = p^s$ où $1 \leq s \leq \alpha$.
   Soit $E = G/S =$ l'ensemble des classes à gauche modulo S.
   On fait opérer P sur E par

$$\begin{array}{ccc} P \times E & \to & E \\ (h, \bar{x}) & \to & \overline{hx} \end{array}$$

   or $E = \bigcup_{k \in K}$ où G_k est une orbite et K un ensemble d'indices.
   Pour un k donné, soit a_k un élément de G_k et H_k le groupe d'isotropie de a_k.
   L'équation aux classes nous dit que $Card(E) = [G : S] = \sum_{k \in K} [P : H_k] = \sum_{k \in K} Card(G_k)$
   $[G : S]$ est premier avec p ; $[P : H_k]$ divise l'ordre de P c'est-à-dire divise p^s et ceci pour tout $k \in K$. Donc $p \mid \sum_{k \in K} [P : H_k]$. Or p est premier avec $[G : S]$ donc p ne divise pas $[G : S]$. Or $Card(E) = [G : S] = \sum_{k \in K} [P : H_k]$ donc l'un des $[P : H_k]$ n'est pas un diviseur propre d'où $\exists k_0 \in K$ tel que $Card(G_{k_0}) = [P : H_{k_0}] = 1$ donc G_{k_0} a un seul élément a_{k_0} donc $G_{k_0} = \{a_{k_0} S\}$.
   Or P opère sur E donc $\forall h \in P$ l'on a : $h\ a_{k_0}\ S = a_{k_0} S$ d'où $\exists (s, t) \in S^2$ tel que $h\ a_{k_0}\ s = a_{k_0}\ t$ donc $h = a_{k_0}\ t\ (a_{k_0}\ s)^{-1}$ d'où $h = a_{k_0}\ t\ s^{-1}\ a_{k_0}^{-1}$.
   Or $t\ s^{-1} \in S$ donc $h \in a_{k_0}\ S\ a_{k_0}^{-1}$ donc $P = a_{k_0}\ S\ a_{k_0}^{-1}$.

P est par conséquent le conjugué T de S . Mais comme S est un $p-$sous-groupe de Sylow alors son conjugué T en est un aussi.

2. On peut faire opérer G par conjugaison sur $\mathcal{H}$ l'ensemble de ses sous-groupes.
   Soit S un $p-$sous-groupe de Sylow de G.
   Soit $\mathcal{S}$ l'orbite de S donc $\mathcal{S} = \{\text{conjugués de S}\}$ Ces conjugués de S sont eux aussi des $p-$sousgroupes de Sylow car S en est un.
   Le stabilisateur de S est l'ensemble des éléments g de G tels que $g\ s\ g^{-1} = S$ donc le stabilisateur de S est le normalisateur de S.
   Par conséquent, $r = card(\mathcal{S}) = \dfrac{Card(G)}{Card(N(S))} = \dfrac{ordre(G)}{Card(N(S))}$ donc $r \mid n = ordre(G)$

3. Soit T un $p-$sous groupe de Sylow de G.
   Si l'on démontre que deux $p-$sous groupes de Sylow sont conjugués, nous répondrons aux deux questions :
   - les $p-$sous-groupes de Sylow de G sont conjugués
   - leur nombre est congru à 1 modulo p. Ce nombre divise n.

   D'après la démonstration du a), comme T est un $p-$sousgroupe alors il existe S un $p-$sous groupe de Sylow de G tel que $T \subset G$.
   D'après la démonstration du a), quelque soit R $p-$sousgroupe de Sylow de G il existe a_{k_0} tel que $R \subset a_{k_0} S a_{k_0}^{-1}$ alors $O(R) = O(a_{k_0} S a_{k_0}^{-1})$ d'où $R = a_{k_0} S a_{k_0}^{-1}$ donc deux $p-$sous groupes de Sylow sont conjugués.
   Par conséquent, $\mathcal{S} = \{\text{p - sous groupes de Sylow}\}$ donc $Card(\mathcal{S}) \mid n$

4. Démontrons que leur nombre est congru à 1 modulo p.
   Faisons opérer S sur $\mathcal{S}$ par conjugaison.
   Soit $P_i \in \mathcal{S}$ et $\mathcal{U}_\rangle$ l'orbite de P_i.
   - Remarquons que $S \in \mathcal{S}$.
     Notons alors $\mathcal{U}$ l'orbite de S donc $\{hSh^{-1}\ h \in S\} \subset \mathcal{U}$ donc $\mathcal{U} = \{S\}$ donc $Card(\mathcal{U}) = 1$ $(*)$
   - Si $Card(\mathcal{U}_i) = 1$ alors $\forall h \in S$ on a $h\ P_i\ \ h^{-1} = P_i$ donc $S \subset N(P_i)$.
     Or S est un $p-$sous groupe de Sylow donc $S \subset P_i$ d'où $S = P_i$ car S est maximal dans les $p-$groupes.
     Par conséquent, si $Card(\mathcal{U}_i) = 1$ alors $P_i = S$ $(**)$
   - D'après $(*)$ et $(**)$ on peut dire que $Card(\mathcal{U}_k) \neq 1$ dès que $S \neq P_i$ donc $Card(\mathcal{S}) = 1 + \sum_i Card(\mathcal{U}_i)$ dès que $P_i \neq S$ d'après l'équation des classes car $Card(Z(G)) = 1$.
     Il reste à prouver que $p \mid \sum_i Card(\mathcal{U}_i)$.

     Or $Car(P_i) = Card(\mathcal{U}_i) \times Card(H_i)$. Or $Card(\mathcal{U}_i) \neq 1$.
     H_i est le stabilisateur de P_i c'est-à-dire $H_i = \{g \in S / gP_ig^{-1} = P_i\}$.
     Comme le stabilisateur est un sous-groupe du groupe qui opère alors $H_i < S$ donc $O(H_i) \mid O(S) = p^{\cdots}$ puisque S est un $p-$sous-groupe de Sylow de G.
     Par conséquent, $Card(H_i) = p^{\cdots}$ et $p \mid Card(P_i)$ donc $Card(P_i) = p^{\cdots}$ donc $Card(\mathcal{U}_i) = p^{\cdots}$.
     On a donc prouvé que $Card(\mathcal{U}_i) \equiv 0\ [p]$ d'où $Card(\mathcal{S}) \equiv 1\ [p]$

4.2.3 Corollaire

Si G n'admet qu'un seul p-sous-groupe de Sylow S alors $S \lhd G$

Démonstration

Comme S est le seul p-sous groupe de Sylow de G et que forcément le conjugué $x\ S\ x^{-1}$ de S est aussi un p-sous groupe de G alors S est son propre conjugué.
Par conséquent, $\forall x \in G$ on a $x\ S\ x^{-1} = S$ donc $x\ S = S\ x$ d'où $S \lhd G$.
CQFD.

4.2.4 Exercice

Soit G un groupe d'ordre 220. Démontrer que G n'est pas simple c'est-à-dire que G a au moins un sous-groupe distingué propre.

Démonstration

On a $220 = 2^2 \times 5 \times 11$. Notons N_{11} le nombre de 11-sous groupes de Sylow de G. Alors $N_{11} \equiv 1\ [11]$ et $N_{11} \equiv 0\ [220]$. Or les nombres congrus à 1 *modulo* 11 sont $1, 12, 23, 34, \cdots$ et les diviseurs de 220 sont : $1, 2, 5, 10, 4, 20$ Par conséquent, $N_{11} = 1$ donc il y a un seul 11-sous groupe S de Sylow de G donc $S \lhd G$. CQFD

Chapitre 5

Groupes Résolubles

5.1 Groupes dérivés

5.1.1 Définition

Soit un groupe G et soient x et y deux de ses éléments.
On appelle **commutateur de x et de y** qu'on note $[x, y]$ l'élément de G défini par :

$$[x, y] = x^{-1}y^{-1}xy$$

On appelle **groupe dérivé de G** qu'on note $D(G)$ le sous-groupe de G engendré par l'ensemble des commutateurs des éléments de G

5.1.2 Théorème

G est commutatif $\iff D(G) = \{e\}$

5.1.3 Théorème

$D(G) \lhd G$ et $\dfrac{G}{D(G)}$ est commutatif

Démonstration

1. Soit ϕ un automorphisme intérieur de G. Alors $\phi([x, y]) = \phi(x^{-1}y^{-1}xy) = \phi(x^{-1})\phi(y^{-1})\phi(x)\phi(y) = (\phi(x))^{-1}(\phi(y))^{-1}\phi(x)\phi(y) = [\phi(x)\phi(y)]$.
   Par conséquent, $D(G)$ est invariant par tout automorphisme intérieur de G donc $D(G) \lhd G$. CQFD.
2. **Idée :**
   Pour prouver que $\dfrac{G}{D(G)}$ est commutatif, on prouvera que $D(\dfrac{G}{D(G)}) = \{\bar{e}\}$.
   $\bar{z} \in D(\dfrac{G}{D(G)}) \iff \bar{z} = [\bar{x}, \bar{y}] = (\bar{x})^{-1}(\bar{y})^{-1}\bar{x}\bar{y} = \overline{x^{-1}y^{-1}xy} = \overline{[x, y]} = \bar{e}$.
   En effet, $[x, y] \in D(G)$ donc $\overline{[x, y]} = \bar{e}$.
   Par conséquent, $D(\dfrac{G}{D(G)}) = \{\bar{e}\}$ donc $\dfrac{G}{D(G)}$ est commutatif .

5.1.4 Exercice

$D(G)$ est le plus petit au sens de l'inclusion sous groupe de G tel que $\frac{G}{K}$ soit commutatif.
c'est-à-dire que si K est tel que $\frac{G}{K}$ soit commutatif alors $D(G) \subset K$.

5.2 Groupes résolubles

5.2.1 Définition

On appelle suite normale d'un groupe G toute suite finie $(G_i)_{i\in[|0;k|]}$ telle que

$$\begin{cases} G_i < G \\ G_0 = G \\ G_k = \{e\} \\ G_{i+1} \lhd G_i \ \forall i \in [\,|\, 0; k-1 \,|\,] \end{cases}$$

c'est-à-dire

$$G_k = \{e\} \lhd G_{k-1} \lhd G_{k-2} \lhd \cdots G_1 \lhd G_0 = G$$

Les groupes quotients $\frac{G_i}{G_{i+1}}$ sont appelés des facteurs de la suite.

5.2.2 Définition

Un groupe G est résoluble s'il admet une suite normale dont les facteurs sont commutatifs.

5.2.3 Notation

$D^0(G) = G; D^1(G) = D(G); \forall n \in \mathbb{N}^*\ D^n(G) = D(D^{n-1}(G))$.

5.2.4 Théorème

1. $D^n(G) \subset D^{n-1}(G) \subset \cdots \subset D(G) \subset G$
2. G est résoluble $\iff \exists n \in \mathbb{N}\ D^n(G) = \{e\}$

Démonstration

1. $D(G) \subset G$.
   Si $D^k(G) \subset G$ alors $D^{k+1}(G) = D(D^k(G)) \subset G$. Or $D(G) \subset G$ donc $D^{k+1} \subset G$.
   On a donc $D^n(G) \subset D^{n-1}(G) \subset \cdots \subset D(G) \subset G$
2. (a) $\Longleftarrow$:
   Supposons qu'il existe $n \in \mathbb{N}$ tel que $D^n(G) = \{e\}$
   donc $\{e\} = D^n(G) \subset D^{n-1}(G) \subset \cdots \subset D(G) \subset G$
   On est donc en présence d'une suite normale dont les facteurs sont commutatifs d'après le théorème précédent donc G est résoluble.

(b) $\Longrightarrow$:
Supposons que G soit résoluble donc $\exists (G_i)_{i\in[|0;k|]}$ telle que

$$G_k = \{e\} \lhd G_{k-1} \lhd G_{k-2} \lhd \cdots G_1 \lhd G_0 = G$$

avec $\dfrac{G_i}{G_{i+1}}$ commutatif. En particulier, $\dfrac{G}{G_1} = \dfrac{G_0}{G_1}$ est commutatif.

- On a $D(G) \subset D(G_1)$.
- Soit $i > 1$. Supposons que $D^i(G) \subset G_i$. Puisque $\dfrac{G_i}{G_{i+1}}$ est commutatif alors $D(G_i) \subset G_{i+1}$ d'où $D^{i+1}(G_i) = D(D^i(G_i))$. Or $D^i(G) \subset G_i$ donc $D^{i+1}(G_i) \subset D(G_i)$ d'où $D^{i+1}(G_i) \subset G_{i+1}$
- Par conséquent, $\forall i \leq k$ l'on a $= D_i(G) \subset G_i$
- On a ainsi prouvé que $D^k(G) \subset G_k = \{e\}$

(c) En conclusion, G est résoluble $\Longleftrightarrow \exists n \in \mathbb{N}\ D^n(G) = \{e\}$

5.2.5 Quelques exemples

Exemple 1

Tout sous groupe H d'un groupe résoluble G est résoluble.

Démonstration :
Supposons que $H < G$ donc $\forall k \in \mathbb{N}$ l'on a $D^k(H) \subset D^k(G)$. Or G est résoluble donc $\exists n \in \mathbb{N}$ tel que $D^n(G) = \{e\}$. Par conséquent $D^n(H) = \{e\}$ donc H est résoluble. CQFD.

Exemple 2

Tout groupe-quotient d'un groupe résoluble est résoluble.

Démonstration :
Soit $H \lhd G$ et soit l'épimorphisme canonique $p : G \longrightarrow \dfrac{G}{H}$.
On vérifie que $p(D^k(G)) = D^k(\dfrac{G}{H})$.
En particulier, $\bar{e} = p(e) = p(D^n(G))$ car G est résoluble.
Donc $\bar{e} = D^n(\dfrac{G}{H})$. Par conséquent, $\dfrac{G}{H}$ est résoluble.

Lemme

Soit f un morphisme du groupe G vers le groupe G'.
Alors la restriction de f à $D(G)$ est noté $D(f)$.

- $D(f)$ est un morphisme de $D(G)$ dans $D(G')$.
- Si f est injective alors $D(f)$ est injective.
- Si f est surjective alors $D(f)$ est surjective.
- Par itération, on construit le morphisme $D^k(f) : D^k(G) \longrightarrow D^k(G')$

Exemple 3

Soit $H \lhd G$ tel que H est résoluble. Si $\frac{G}{H}$ est résoluble alors G est résoluble.

Démonstration :

Supposons que $\frac{G}{H}$ soit résoluble alors $\exists n \in \mathbb{N}^*$ tel que $D^n(\frac{G}{H}) = \{\bar{e}\}$.
Soit le morphisme surjectif $p : G \longrightarrow \frac{G}{H}$.
On construit alors le morphisme surjectif $D^n(p) : D^n(G) \longrightarrow D^n(\frac{G}{H}) = \{\bar{e}\}$.
Par conséquent, $D^n(G) \subset ker(D^n(p) \subset \cdots \subset ker(p) = H$.
Or H est résoluble donc $\exists m \in \mathbb{N}^*$ tel que $D^m(H) = \{e\}$.
On en déduit que $D^{n+m}(G) \subset D^m(H) = \{e\}$.
Par conséquent, $D^{n+m}(G) = \{e\}$ donc G est résoluble.

5.3 Résolubilité des groupes symétriques

5.3.1 Groupe symétrique

Définition

> Soit E un ensemble. On appelle permutation de E toute bijection de E dans E. On appelle S_E leur ensemble.

Propriété

> $(S_E,\ o\ )$ est un groupe appelé groupe symétrique de E.
> Ce groupe n'est pas commutatif pour $n \geq 3$.

Lemme

> S'il existe une bijection f de E dans F alors $S_E \simeq S_F$.

Démonstration :
Il suffit de construire l'application

$$\begin{array}{rccc} \phi : & S_E & \longrightarrow & S_F \\ & s & \mapsto & \phi(s) = s\ o\ f\ o\ s^{-1} \end{array}$$

qui est un isomorphisme de S_E sur S_F.

Définition

On note S_n l'ensemble des permutations de $[\![1; n]\!]$

Théorème

Si $Card(E) = n$ alors $S_E \simeq S_n$

Théorème

$Card(S_n) = n!$

Théorème

1. Toute permutation différente de Id est décomposable en produit de cycles de supports disjoints.
2. Les seules permutations involutives sont les cycles d'ordre 1 et les cycles d'ordre 2 (ou transpositions).
3. Toute permutation est décomposable en produit de transpositions c'est-à-dire que S_n est engendré par les transpositions.
4. Mieux toute permutation est décomposable en produit de transpositions particulières $\tau_{i,i+1}$.
5. (a) Il existe un morphisme surjectif et un seul appelé signature :

$$\varepsilon : groupe\ (S_n,\ o\ ) \longrightarrow groupe\ (\{-1; +1\}, \times)$$

tel que $\varepsilon(\tau) = -1$ pour toute transposition τ

(b) $A_n = ker(\varepsilon)$ est un sous groupe distingué de S_n, appelé le groupe alterné.

(c) A_n est engendré par les permutations paires c'est-à-dure les permutations qui sont les composées de deux transpositions.

(d) A_n est aussi engendré par les cycles de longueur 3 de S_n.

(e) pour tout $n \leq 5$, A_n est un groupe simple.

Ordre d'une permutation

- Soit $\tau = (i, j)$ une transposition c'est-à-dire un 2-cycle dans S_n alors $ordre(\tau) = 2$ car $\tau^2 = \tau \circ \tau = (i, j)(i, j) = id$
- L'ordre d'un $3-$cycle (a, b, c) dans S_n est 3 car $(a, b, c)^3 = (a, b, c)(a, b, c)(a, b, c) = id$
- L'ordre de la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$ est 6

  car $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$

  $\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$ $\quad$ $\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}$

$$\sigma^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \qquad \sigma^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = id$$

- On peut retrouver ce dernier résultat en décomposant σ en produit commutatif de cycles de supports disjoints :
  $\sigma = (1,3)(2,5,4)$
  $\sigma^2 = (1,3)(2,5,4)(1,3)(2,5,4) = (1,3)^2(2,5,4)^2 = id \circ (2,4,5) = (2,4,5)$
  $\sigma^3 = (1,3)^3(2,5,4)^3 = (1,3) \circ id = (1,3)$
  $\sigma^4 = (1,3)^4(2,5,4)^4 = (1,3) \circ (2,5,4) = (2,5,4)$
  $\sigma^5 = (1,3)^5(2,5,4)^5 = (1,3) \circ (2,5,4)^2 = (1,3)(2,4,5)$
  $\sigma^6 = (1,3)^3(2,5,4)^6 = id \circ id = id)$
  Quand on met une transposition à une puissance paire, elle disparaît car elle devint l'identité. Idem si l'on met le 3-cycle à une puissance multiple de 3.
  Par conséquent lorsque l'on aura le ppcm de 2 et 3 c'est-à-dire l'on aura l'ordre de σ

Théorème

L'ordre d'un $k-$cycle $\sigma = (i_1, i_2, \cdots, i_k)$ est k.

Démonstration :

- $\sigma(i_1) := i_2 \neq i_1; \sigma^2(i_1) := i_3 \neq i_1; \cdots; \sigma^{k-1}(i_1) := i_k \neq i_1$ donc $ord(k) \geq k$
- Mais $\sigma^k(i_1) = i_1$
- C'est pareil pour $i_2, \cdots, i_k$ donc $\sigma^k = id$ d'où $ordre(\sigma) = k$

Exercice

Déterminer l'ordre de la permutation :
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \\ 4 & 1 & 7 & 6 & 9 & 8 & 1 & 3 & 2 & 5 \end{pmatrix}$

$\sigma = (1,4,6,8,2)(3,7)(5,9)$ donc $\sigma^p = (1,4,6,8,2)^p(3,7)^p(5,9)^p$.
L'ordre du $5-$cycle est 5 et l'ordre de chacune des deux transpositions est 2.
Par conséquent, $\sigma^p = id \iff p$ est un multiple de 5 et p est pair car
Donc $ordre(\sigma) = 10$.

Corollaire : Ordre d'une permutation

Comme une permutation σ se décompose en produit de cycles de supports disjoints :
$\sigma = \gamma_1\gamma_2 \cdots \gamma_m$ alors :
$ordre(\sigma) = ppcm(k_1, k_2, \cdots, k_m)$ où $ordre(\gamma_i) = k_i$

5.3.2 Théorème

S_E opère sur E par l'application :

$$\begin{array}{rccc} \phi : & S_E \times E & \longrightarrow & E \\ & (s,x) & \mapsto & \phi(s) = s(x) \end{array}$$

5.3.3 Théorème

Si $n \leq 5$ alors S_n n'est pas résoluble.

Démonstration

Soient deux cycles de longueur 3 $\sigma = (i,j,k)$ et $\rho = (k,r,s)$ où i,j,k,r et s soient deux à deux distincts, il faut $n \geq 5$ d'où l'hypothèse $\sigma^{-1} = (i,k,j)$ et $\rho^{-1} = (k,s,r)$ donc $\sigma\rho\sigma^{-1}\rho^{-1} = (i,r,k)$.
Par conséquent, $[\sigma,\rho] \in A_n$ car A_n est engendré par les cycles de longueur 3. On a donc $D(A_n) = A_n$ d'où $\forall k \in \mathbb{N}^*$ l'on a : $D^k(A_n) = A_k$

- Or $A_n \subset D_n$ donc $D(A_n) \subset D(S_n)$
- $D(S_n) \neq \{id_E\}$ sinon S_n serait commutatif.
- Si $n > 3$ on a $D(A_n) \neq \{id_E\}$ sinon A_n serait commutatif.

Par conséquent, $\forall k \in \mathbb{N}^*$ l'on a : $\{id_E\} \neq D^k(A_n) \subset D(S_n)$ donc S_n n'est pas résoluble.

5.3.4 Théorème

S_2, S_3 et S_4 sont résolubles.

Chapitre 6

Groupes d'ordre $n \leq 15$ et $n \neq 12$

6.1 Les groupes diédraux

6.1.1 Définition

Pour tout $n \in \mathbb{N}$, il existe , à un isomorphisme près, un seul groupe d'ordre $2n$ engendré par deux de ses éléments r et s tels que

1. r est d'ordre n.
2. s est d'ordre 2.
3. sr est d'ordre 2.

Ce groupe est appelé *groupe diédral* d'ordre $2n$ et est noté Δ_n.

6.1.2 Remarques

La condition 3 peut s'écrire $(sr)(sr) = e$ ou encore $srs = r^{-1}$

Cas $n = 1$

Si $n = 1$ les trois relations précédentes s'écrivent :

1. r est d'ordre 1 c'est-à-dire $r = e$
2. s est d'ordre 2 c'est-à-dire $s^2 = e$.
3. sr est d'ordre 2 c'est-à-dire $srsr = e$.

Donc $r = e$ et $s^2 = e$ et $\Delta_1 = C_2 =$ le groupe cyclique d'ordre 2.

Cas $n = 2$

Si $n = 2$ les trois relations précédentes s'écrivent :

1. r est d'ordre 2 c'est-à-dire $r^2 = e$
2. s est d'ordre 2 c'est-à-dire $s^2 = e$.
3. sr est d'ordre 2 c'est-à-dire $srsr = e$.

Donc $sr = rs$ et Δ_2 est commutatif étant engendré par deux éléments qui commutent.
Par conséquent, $\Delta_2 = C_2 \times C2 =$ *le groupe de Klein* qui est un groupe d'ordre 4.

6.1.3 Théorème

S_n est commutatif $\Longleftrightarrow n \leq 2$.

Démonstration

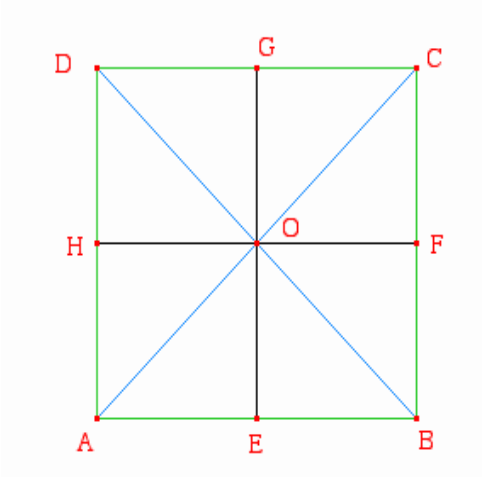
$\Longleftarrow$:
évident.
$\Longrightarrow$:
2 cas

- *npair*
- *nimpair*

6.1.4 Remarque

Le groupe diédral Δ_n est aussi le groupe des isométries laissant invariant un polygone régulier de n côtés.

Cas $n = 4$



On note $a = Rot(0, \frac{\pi}{2}); b = Rot(0, \pi); c = Rot(0, \frac{3\pi}{2}); d = Sym(EG); e = Id_E; f = Sym(FH); g = Sym(AC); h = Sym(BD)$
$\Delta_4 = \{a, b, c, d, e, f, g, h\}$ muni de la loi o de composition des applications

Voici la table de Δ_4 :

o	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
a					a			
b					b			
c					c			
d					d			
e	a	b	c	d	e	f	g	h
f					f			
g					g			
h					h			

6.2 Le groupe quatertionique M

On sait que tout sous groupe d'un groupe abélien est normal ou distingué.

1. Existe-t-il des groupes non abéliens dont tous les sous groupes propres sont distingués ?

   (a) Oui, le plus petit groupe non abélien vérifiant cette propriété a été mis en évidence par HAMILTON : c'est le groupe quatertionien M d'Hamilton. Il est d'ordre 8.

   (b) M est engendré par deux éléments $a \neq b$ vérifiant la relation

   $$a^2 = b^2 = (ab)^2 \neq e$$

   (c) $M = \{a, b, ab, ba, a^2, a^3, b^3\}$

   (d) On démontre que $a^4 = b^4 = e$

   (e) On peut prendre aussi comme relations de définition :

   $$a^4 = e; a^2 = b^2 \neq e; aba = b \; ou \; bab^{-1} = a^{-1}$$

   (f) Tous les sous groupes de M sont distingués.

2. Existe-t-il des groupes non abéliens dont aucun sous groupe propre n'est distingué ? Oui, le plus petit groupe non abélien vérifiant cette propriété est d'ordre 60 et s'appelle le groupe Icosaedral. Il a été trouvé par Evariste GALOIS.

6.3 Propriétés

6.3.1 Théorème

Le centre $Z(M)$ est d'ordre 2 et $\dfrac{M}{Z(M)} \simeq C_2 \times C_2$.

Démonstration

On sait que $O(M) = 2^3$ donc est de la forme p^3 où p est 1^{er}.
Or $O(Z(M)) = 2 = p$ et on sait que $\dfrac{G}{Z(G)} \simeq C_p \times C_p$.

Par conséquent, $\dfrac{M}{Z(M)} \simeq C_2 \times C_2$. CQFD.

6.3.2 Théorème

> Soit p un entier premier ≥ 3 alors tout groupe G d'ordre $2p$ est soit cyclique soit diédral.
> Ce qui est le cas par exemple pour $6 = 2 \times 3; 8 = 2 \times 4; 10 = 2 \times 5; 14 = 2 \times 7$

Démonstration

Soit n_2 le nombre de $2-$sous groupes de Sylow de G.
Soit n_p le nombre de $p-$sous groupes de Sylow de G.

1. On sait que $n_p \equiv 1\ [p]$ et que $n_p \mid 2p$ donc comme $n_p \geq 0$ on a $n_p = 1$ ou $n_p = 2p$.
   Or $n_p \equiv 1\ [p]$ donc $n_p = 1$
   Soit S_p l'unique $p-$sous groupe de Sylow de G. On a $S_p \lhd G$.
2. On sait que $n_2 \equiv 1\ [2]$ et que $n_2 \mid 2p$ donc comme $n_2 \geq 0$ on a $n_2 = 1$ ou $n_2 = p$.

   - **ou** $n_2 = 1$
     Soit S_2 l'unique $2-$sous groupe de Sylow de G. On a $S_2 \lhd G$ donc $S_2S_p < G$ et $O(S_2S_p) = 2p$ car $S_2S_p = \{e\}$ car $\forall x \in S_2$ l'on a : $x^2 = e$ et $\forall x \in S_p$ l'on a : $x^p = e$. Or $pgcd(2; p) = 1$ Donc comme $O(G) = 2p$ alors $G \simeq S_2 \bigoplus S_p$ ou $G \simeq S_2 \times S_p$.
     Or 2 est 1^{er} donc $S_2 \simeq C_2$ et $S_p \simeq C_p$ par conséquent $S_2 \times S_p \simeq C_2 \times C_p$.
     Or $C_2 \times C_p \times C_p$ car $pgcd(2; p) = 1$ donc $G \simeq C_p$ donc G est cyclique.CQFD.
   - **ou** $n_2 = p$
     alors $[G : S_p] = 2$. Or tout sous groupe d'indice 2 est distingué donc $G = S_p \cup sS_p$ où $s \in G$ et $s \notin S_p$.
     $O(S_p) = p$ où $p1^{er}$ donc S_p est cyclique. Soit r le générateur de S_p donc $r^p = e$.
     On sait que $O(r) = p$ car $r^p = e$ et $r \neq e$.
     Quel est l'ordre de s ?

     — ou bien $O(s) = 2p$ alors $G = (s)$ donc G est cyclique donc abélien.
     Soient S et T deux sous groupes de Sylow de G.
     On sait que S et T sont conjugués donc $\exists x \in G$ tel que $T = xSx^{-1}$.
     Or G est abélien donc $xSx^{-1} = S$ donc $n_2 = 1$ Ceci est faux car $n_2 = p \neq 1$.
     — ou bien $O(s) = 1$ donc $s = e$. Or $e \in S_p$ et $s \notin S_p$ donc cette hypothèse est fausse.
     — ou bien $O(s) = p$. Soit $T = (s)$ donc $O(T) = p$ donc T est un $p-$sous groupe de Sylow de G car 1 est la puissance maximum.
     Or $T \neq S_p$ car $s \notin S_p$. Mais il n'y a qu'un seul $p-$sous groupe de Sylow car $n_p = 1$ donc il est impossible d'avoir $O(s) = p$.

— Par conséquent, $O(s) = 2$. Une démonstration analogue nous permet d'affirmer que sr est d'ordre 2 donc G est Δ_p. CQFD.

6.3.3 Théorème

Δ_4 et M ne sont pas isomorphes.

Démonstration

Δ_4 a au moins deux éléments d'ordre 2 qui sont s et r^2 alors que M n'a qu'un seul élément d'ordre 2.

6.3.4 Théorème

Tout sous groupe d'ordre 8 est soit abélien, soit isomorphe à Δ_4 ou à M

Démonstration à revérifier ! ! !

1. ou bien G est abélien. CQFD.
2. ou bien G n'est pas abélien.
   Comme $O(G) = 8$ alors l'ordre d'un élément de G est soit 1 soit 2 soit 4 ou soit 8.
   - Supposons que G ne contienne aucun élément d'ordre 4.
     — Supposons que $\forall x \in G\ O(x) = 1$ mais alors $G = \{e\}$ donc G serait abélien. Impossible.
     — Supposons que $\forall x \in G\ O(x) = 2$ mais alors G serait abélien. Impossible.
     — Supposons que $\forall x \in G\ O(x) = 8$ donc $x^8 = e$ donc $(x^4)^2 = e$ donc il y aurait x^4 d'ordre 2. Cela n"est pas possible.
   - Par conséquent G a au moins un élément a d'ordre 4. Soit $H = (a)$ alors $O(H) = 4$ et $[G : H] = 2$ donc $H \lhd G$.
     Par conséquent, $G = H \cup bH$ où $b \notin H$. Mais alors $b^2 \notin bH$ car si $\exists h \in H\ b^2 = bh$ alors $b = h$ donc $b \in H$ impossible. Donc $b^2 \notin bH$ d'où $b^2 \in H$.
   - $H \lhd G$ donc $bab^{-1} \in H$ car $a \in H$. Donc $(bab^{-1})^4 = bab^{-1}bab^{-1}bab^{-1}bab^{-1} = ba^4b^{-1} = beb^{-1} = e$
   - Si $k \in \{2; 3\}$ alors $(ba^4b^{-1})^k \neq e$ car $a^k \neq e$ puisque $a^2 \neq e$ et $a^3 \neq e$.
   - Par conséquent, ba^4b^{-1} est d'ordre 4 donc $H = \{e; a; a^2; a^3 = a^{-1}\}$ et $O(a^2) = 2$ puisque $a \neq e$ et $(a^2)^2 = a^4 = e$
   - Donc bab^{-1} est soit a soit a^{-1}
   - ou $bab^{-1} = a$ donc $ba = ab$. Deux éléments de H commutent et que $H = (a)$. De plus, deux éléments de bH commutent car $ab = ba$. Tout élément de H commute avec tout élément de bH. Par conséquent, comme $G \subset H \cup bH$ alors G est abélien. Ce qui est impossible.
   - Donc $bab^{-1} = a^{-1}$.L'ordre de b est donc $1, 2, 4$ ou 8.
   - ou $O(b) = 8$ mais alors $G = (b)$ donc G est cyclique donc abélien. Impossible.
   - ou $O(b) = 1$ alors $b = e$donc $b \in H$. Impossible.
   - Donc $O(b) = 2$ ou $O(b) = 4$ donc $b^4 = e$. Donc $b^4 \in H = \{e; a; a^2; a^3 = a^{-1}\}$ donc

— ou $b^2 = e$
alors G est engendré par 2 éléments a et b tels que

$$\begin{cases} a^4 = e \\ b^2 = e \\ bab^{-1} = a^{-1} \end{cases}$$

donc $G \simeq \Delta_4$
— ou $b^2 = a^2$ alors G est engendré par 2 éléments a et b tels que

$$\begin{cases} a^4 = e \\ b^2 = a^2 \\ bab^{-1} = a^{-1} \end{cases}$$

donc $G \simeq M$

6.3.5 Théorème

> Tout groupe G d'ordre 15 est cyclique.

Démonstration

Soit n_3 le nombre de 3−sous groupes de Sylow de G.
Soit n_5 le nombre de 5−sous groupes de Sylow de G.
Alors $n_3 \equiv 1$ [3] et $n_3 \mid 15$ donc $n_3 = 1$.
De même $n_5 \equiv 1$ [5] et $n_5 \mid 15$ donc $n_5 = 1$
Par conséquent, soit S_3 l'unique 3−sous groupe de Sylow de G où $S_3 \lhd G$ et soit S_5 l'unique 5−sous groupe de Sylow de G où $S_5 \lhd G$.
Donc $S_3S_5 < G$ avec $O(S_3S_5) = 15$ car $S_3 \cap S_5 = \{e\}$.
On en déduit que $G \simeq S_3 \times S_5 \simeq C_3 \times C_5$ car $3 \wedge 5 = 1$ donc $G \simeq C_{15}$.

6.4 Classification

Ordre	*Groupes*
2	C_2
3	C_3
$4 = 2 \times 2$	$C_2 \times C_2; C_4$
5	C_5
$6 = 2 \times 3$	C_6
7	C_7
$8 = 4 \times 2$	$C_8; C_4 \times C_2; C_2 \times C_2 \times C_2; \Delta_4; M$
$9 = 3 \times 3$	$C_3 \times C_3$
$10 = 2 \times 5$	$C_10; \Delta_5$
11	C_{11}
13	C_{13}
$14 = 2 \times 7$	C_{14}
15	C_{15}

Chapitre 7

Groupe des isométries laissant invariant un ensemble donné

7.1 Stratégie de recherche

7.1.1 Définition

Soit E un espace affine. Soit F un sous ensemble non vide de E.
Soit f une isométrie de E.
On dit que F est invariant par f lorsque $f < F >= F$

7.1.2 Théorème

1. L'ensemble $\mathcal{J}_F$ des isométries de E laissant F invariant est un sous-groupe du groupe $(\mathcal{J}_E, \circ)$ des isométries de E.
2. L'ensemble $\mathcal{J}_F^+$ des déplacements de E laissant F invariant est un sous-groupe du groupe $(\mathcal{J}_F, \circ)$ des isométries de E laissant F invariant.

Démonstration évidente.

7.1.3 Propriété

Si une isométrie f laisse invariant un ensemble fini de points alors f laisse invariant l'isobarycentre G de cet ensemble de points.

Comme f est une isométrie alors f est une application affine donc f conserve le barycentre.

7.1.4 Stratégie

Pour déterminer l'ensemble des isométries qui conservent un ensemble donné, on utilise le théorème précédent ainsi que les théorèmes qui suivent.

7.2 Groupe G des déplacements de E_3 conservant un point O

G est l'ensemble des rotations d'axe des droites (D) passant par O

7.3 Groupe des déplacements de E_2 conservant un point O

G est l'ensemble formé :
- des déplacements suivants : les rotations de centre O
- des antidéplacements suivants : les symétries orthogonales d'axes les droites passant par O

7.4 Groupe des déplacements de E_2 conservant la paire $\{A; B\}$

G est l'ensemble formé :
- des 2 isométries transformant A en A et B en B :
  Id_{E_2} et la symétrie orthogonale $S_{(AB)}$
- des 2 isométries transformant A en B et B en A :
  la symétrie centrale S_O et la symétrie orthogonale S_Δ
  où O est le milieu de $[AB]$ Δ est la médiatrice de $[AB]$.

La table de ce groupe est :

$\circ$	Id	S_D	s_Δ	S_O
Id	Id	S_D	s_Δ	S_O
S_D	S_D	Id	S_O	s_Δ
s_Δ	s_Δ	S_O	Id	S_D
c	S_O	s_Δ	S_D	Id

Ce groupe est un groupe de KLEIN où chaque élément est son propre symétrique.

7.5 Groupe des déplacements de E_2 conservant un triangle équilatéral $\{A, B, C\}$

1. Ce groupe $\mathcal{J}_{\{A,B,C\}}$ est inclus dans le groupe $\mathcal{S}_{\{A,B,C\}}$ des permutations de l'ensemble $\{A, , B, C\}$ donc $Card(\mathcal{J}_{\{A,B,C\}}) \leq 3! = 6$

2. Si f est une isométrie laissant invariant l'ensemble $\{A,,B,C\}$ alors f laisse invariant l'isobarycentre G de ces trois points.
3. Par conséquent f est
   - Soit Id (déplacement)
   - Soit une rotation de centre G et d'angle non nul.(déplacement)
   - Soit une symétrie orthogonale d'axe une droite passant par G (antidéplacement)

La table de ce groupe est :

$\circ$	Id	S_{GA}	S_{GB}	S_{GC}	$R_1\left(G,\frac{2\pi}{3}\right)$	$R_2\left(G,\frac{4\pi}{3}\right)$
Id	Id	S_{GA}	S_{GB}	S_{GC}	R_1	R_2
S_{GA}	S_{GA}	Id	R_1	R_2	S_{GB}	S_{GC}
S_{GB}	S_{GB}	R_2	Id	R_1	S_{GC}	S_{GA}
S_{GC}	S_{GC}	R_1	R_2	Id	S_{GA}	S_{GB}
$R_1\left(G,\frac{2\pi}{3}\right)$	R_1	S_{GC}	S_{GA}	S_{GB}	R_2	Id
$R_2\left(G,\frac{4\pi}{3}\right)$	R_2	S_{GB}	S_{GC}	S_{GA}	Id	R_1

Ce groupe non commutatif comporte 6 éléments et est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ par le théorème des restes chinois. Ce sont tous deux des groupes cycliques

7.6 Groupe des Isométries conservant un carré

Ce groupe comporte 8 éléments, et on peut alors se demander s'il est isomorphe à $\mathbb{Z}/8\mathbb{Z}$ ou a $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ ou a $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. L'isomorphisme n'est pas avec $\mathbb{Z}/8\mathbb{Z}$ qui comporte un élément d'ordre 8 mais avec $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ (le groupe des isométries du cube comporte une rotation d'ordre 4, et tous ses éléments peuvent s'écrire comme la composée d'une rotation et d'une éflexion, et enfin on remarque que $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ n'a pas éléments d'ordre 4)....

7.7 Bibliographie

Analyse combinatoire - Louis Comtet
La fascination des groupes
La classification des groupes finis simples - Daniel Lignon - Bulletin Apmep 334 Juin 82