Chapitre 13

Groupes

Résumé -

Comme structure algébrique, nous devons étudier les groupes (une seule loi, interne), les anneaux et corps (deux lois internes) et les espaces vectoriels (deux lois internes et une externe). Nous parlerons sûrement à l'occasion d'algèbre et sûrement d'espace affine.
Le chapitre qui suit est assez court, et se concentre sur la structure de groupes.
La notion de groupe a été formalisée au début du XIX-ième siècle mais n'a trouvé toute sa force qu'à la fin du siècle. Nous préparerons quelques notions de seconde année. Et nous reprendrons cette notion en étudiant au second semestre le groupe des permutations, et ensuite nous verrons agir des groupes sur les matrices carrées.

— *Michaël Launay - Structure algébrique - https ://www.youtube.com/watch?v=RaqlxOihGxw*
— *PoincareDuality - « Les maths ne sont qu'une histoire de Groupe » Poincaré par Etienne Ghys - https ://www.youtube.com/watch?v=dLwi_opxLxs*
— *Interview Cirm - Claire voisin - https ://www.youtube.com/watch?v=vcwMTpgNlQA*

Sommaire

1. Problèmes

? Problème 59 - Structure

En MPSI, la recherche de la démonstration, optimale la plupart du temps conduit à réfléchir précisément sur les hypothèses qui permet d'obtenir les résultats. Ainsi les objets sont épurés sur les hypothèses principales.
De quel ensemble et avec quelle loi (structure) minimale doit-on partir pour l'essentiel de nos théorèmes à l'origine ?

? Problème 60 - Résolution des équations polynomiales

Comment démontrer qu'en règle générale, un polynôme de degré 5 n'admet pas de formules explicites des racines du polynôme ?
C'est l'une des questions qui a conduit GALOIS à créer (inventer, découvrir) la notion de groupe... Quel chemin l'a conduit à cette construction ?

Histoire - Evariste Galois

La vie (très courte et très romantique) d'Evariste Galois (1811-1832) pourrait faire la base d'un excellent film...
On le présente souvent comme le premier, avec de nombreuses années d'avance, qui a compris le rôle fondamental de la structure de lois internes et de groupe. Il a ainsi démontré que pour $\geqslant 5$, il n'existe pas de formule explicite et avec des racines n^e exprimant les racines d'un polynôme quelconque de degré n.

? Problème 61 - Groupe de Poincaré

En physique relativiste, les éléments de l'espace sont des quadruplets (x, y, z, t).
On appelle groupe de Poincaré l'ensemble $(G, \circ)$ des transformations $\varphi : \mathbb{R}^4 \to \mathbb{R}^4 \in G$ tel que pour tout paire de quadruplets (x, y, z, t) et (x', y', z', t'), la distance est conservée :
$(x-x')^2+(y-y')^2+(z-z')^2-c^2(t-t')^2 = (X-X')^2+(Y-Y')^2+(Z-Z')^2-c^2(T-T')^2$
où $\varphi(x, y, z, t) = (X, Y, Z, T)$ et $\varphi(x', y', z', t') = (X', Y', Z', T')$.
Montrer qu'il s'agit bien d'un groupe.

? Problème 62 - Mariage chez les Murngin (citation)

A New York, [Lévi-Strauss] s'était lancé dans un vaste travail de sociologie théorique qui devint sa thèse de doctorat (aujourd'hui célèbre) sur les structures ?élémentaires de la parenté. Un jour, dans l'étude d'un certain type de mariage, il se heurta à des difficultés inattendues et pensa qu'un mathématicien pourrait lui venir en aide.
D'après ce qu'ont observé les sociologues travaillant? sur le terrain?, les lois de mariage des tribus indigènes d'Australie comportent un mélange de règles exogamiques et endogamiques dont la description et l'étude posent des problèmes combinatoires parfois compliqués. Le plus souvent le sociologue s'en tire par l'énumération de tous les cas possibles dans l'intérieur d'un système donné. Mais la tribu des Murngin, à la pointe Nord de l'Australie, s'était donné un système d'une telle ingéniosité que Lévi-Strauss n'arrivait plus à en dérouler les conséquences. En désespoir de cause il me soumit son problème.
Le plus difficile pour le mathématicien, lorsqu'il s'agit de mathématique appliquée, est souvent de comprendre de quoi il s'agit et de traduire dans son propre langage les données de la question. Non sans mal, je finis par voir que tout se ramenait à étudier deux permutations et le groupe qu'elles engendrent. Alors apparut une circonstance imprévue. Les lois de mariage de la tribu Murngin, et de beaucoup d'autres, comportent le principe suivant : ? Tout homme peut épouser la fille du frère de sa mère ? ou, bien entendu, l'équivalent de celle-ci dans la classification matrimoniale de la tribu. Miraculeusement, ce principe revient à dire que les deux permutations dont il s'agit sont échangeables, donc que le groupe qu'elles engendrent est abélien. Un système qui à première vue menaçait

> d'être d'une complication inextricable devient ainsi assez facile à décrire dès lors qu'on introduit une notation convenable. Je n'ose dire que ce principe a été adopté pour faire plaisir aux mathématiciens, mais j'avoue qu'il m'en est resté une certaine tendresse pour les Murngin.
> Oeuvres scientifiques, André Weil, 1979 p. 567-568

2. Lois de composition internes

2.1. Définitions

Définition - Loi de composition interne (Magma)
Une loi de composition interne sur un ensemble E est une application de $E \times E$ dans E : $\Phi : E \times E \to E, (x, y) \mapsto x \star y$.
On note, pour $(x, y, z) \in E^3$,
$(x \star y) \star z = \Phi(\Phi(x, y), z)$ et $x \star (y \star z) = \Phi(x, \Phi(y, z))$.
Un tel couple $(E, \star)$ est appelé un magma.
Quand la loi interne est clairement identifiée, par abus, on peut dire que E est un magma sans précision supplémentaire.

Exemple - $\mathbb{N}$

Définition - Caractéristiques
On dit que le magma $(E, \star)$:
- est commutatif si $\forall (x, y) \in E \times E$, $x \star y = y \star x$
- est associatif si $\forall (x, y, z) \in E \times E \times E$, $x \star (y \star z) = (x \star y) \star z$
- est unifère ou possède un élément neutre s'il existe $e \in E$ tel que $\forall x \in E$, $e \star x = x \star e = x$ (e est alors l'élément neutre.)

Pour x élément de E, on dit qu'un élément y de E est un symétrique ou un inverse de x pour $\star$ si $x \star y = y \star x = e$, ($e$ neutre de E)

Définition - Monoïde
Un magma $(M, \star)$ associatif et unifère est appelé un monoïde.

Remarque - Notations
Plusieurs remarques
1. Les lois de composition interne sont usuellement notées $\star$, $\perp$, $\top$, $+$, $\times$, en notation multiplicative $x \star y = xy$.
2. La notation additive est usuellement réservée à une loi commutative et associative, dans ce cas le symétrique de x (s'il existe) est noté $-x$.
3. Lorsque la loi est commutative et associative, on peut écrire :
$$\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n \text{ (notation additive) } ou \prod_{i=1}^{n} x_i = x_1 \dots x_n \text{ (notation multiplicative).}$$
4. Si la loi $\star$ est associative, on peut écrire $x^{\star n} = x \star \cdots \star x$ (n termes x). En notation multiplicative on obtient ainsi x^n et en notation additive nx.

Définition - Distributivité
Supposons que l'ensemble E est muni de deux lois internes $\star$ et $\top$.
On dit que $\star$ est distributive par rapport à la loi interne $\top$ si :
$\forall (x, y, z) \in K^3$, $x \star (y \top z) = (x \star y) \top (x \star z)$ (distibutive à gauche)
$\forall (x, y, z) \in K^3$, $(x \top y) \star z = (x \star z) \top (y \star z)$ (distibutive à droite)

2.2. Propriétés directes

Proposition - Unicités (éléments neutres, symétrique)... si existence
Soit $(F, \top)$ un magma.
Si F est unifère, l'élément neutre pour $\top$ est unique.
Soit $(E, \star)$ un monoïde.
Si $x \in E$ admet un symétrique alors celui-ci est unique;
Si $x, y \in E$ admettent des symétriques x^{-1} et y^{-1}
alors $x \star y$ admet un symétrique : $y^{-1} \star x^{-1}$.
Si x est symétrique alors x est régulier (à gauche et à droite) :
$\forall\ y, z \in E,\ x \star y = x \star z \Rightarrow y = z$ et $y \star x = z \star x \Rightarrow y = z$.

Démonstration

2.3. Induction

Il s'agit de l'induction de la loi sur une partie ou une restriction d'un magma E.

Définition - Loi induite
Soit $A \subset E$, avec $(E, \top)$ magma.
A est stable par $\top$ (loi de composition interne sur E) si $\forall x, y \in A$, $x \top y \in A$.
$\top_A = \top_{|A \times A}$ s'appelle la loi induite (par $\top$ sur A).

Remarque - Transmission des propriétés
$\top_A$ est alors une loi interne sur A, i.e. $(A, \top_A)$ est un magma (induit).
Si $\top$ est commutative (resp. associative), $\top_A$ est nécessairement commutative (resp. associative).
En revanche l'élément neutre de $\top$ ou l'élément symétrique de $x \in A$ pour $\top$ (s'ils existent) ne sont pas nécessairement dans A.

3. Structure de groupe

3.1. Définition et propriétés

Un groupe est un monoïde dont tous les éléments sont inversibles :

Histoire - Plusieurs naissances
En fait, cela est comme toujours plus subtil. Il semble que l'idée de groupe est en germe à la fin du XVIII siècle (en particulier chez Lagrange) et donc le concept apparait clairement ensuite mais à plusieurs endroits en même temps : chez Galois en France, dans les écrits de Cayley en Grande Bretagne ou dans les

Définition - Groupe
On appelle groupe un ensemble G muni d'une loi de composition interne $\top$ vérifiant :
- la loi $\top$ est associative ;
- G possède un élément neutre pour $\top$;
- tout élément x de G possède un symétrique pour $\top$ (ou tout élément de G est inversible, est symétrisable).

Si de plus la loi $\top$ est commutative, on dit que le groupe est abélien (ou commutatif).

Exemple - Groupes des racines de l'unité

Remarque - Sous-groupe
Finalement, on a utilisé ici le fait que $(\mathbb{C},\times)$ était lui même un groupe, que $\mathbb{U}$ est stable par la loi induite, que $1_{\mathbb{C}} \in \mathbb{U}$ et pour tout $z \in U(\subset \mathbb{C})$, $\frac{1}{z}(\in \mathbb{C}) \in \mathbb{U}$.
On reviendra sur ces propriétés plus loin.

Proposition - Régularité
Dans un groupe tous les éléments sont réguliers à gauche et à droite

Démonstration

Comme des groupes sont des magmas unifère, où tous les éléments sont inversibles par définition :

Théorème - Existence et unicité
Soit $(G,\top)$ un groupe. Alors :
- L'élément neutre est unique.
- Tout élément possède un unique symétrique.
- En notant x^{-1} le symétrique (l'inverse) de x, on a $(x^{-1})^{-1} = x$.
- $(x\top y)^{-1} = y^{-1}\top x^{-1}$.

3.2. Groupes produits

Définition - Produit de groupes
Soient $(G,\perp)$ et $(H,\top)$ deux groupes.
On appelle groupe produit (de ces deux groupes) le groupe $(G\times H,\star)$ tel que

$$\forall\ (x_1,y_1),(x_2,y_2) \in G\times H,\qquad (x_1,y_1)\star(x_2,y_2) = (x_1\perp x_2, y_1\top y_2)$$

Pour aller plus loin - Produit direct. Produit indirect
En réalité, le produit comme il apparait ici est souvent qualifié de produit direct.
Le produit semi-direct est alors le produit de décomposition d'un groupe G sous la forme $G = HK$, où H est un sous-groupe normal ou distingué de G et K est isomorphe à $\frac{G}{H}$.

Il s'agit bien d'un groupe :

Démonstration

Remarque - Souvent $G = H$
On considère donc le groupe produit noté$(G^2, \perp)$ plutôt que $(G^2, \perp^2)$.
Et par récurrence, on peut étendre le produit de groupes à plus de deux groupes.

3.3. Exemples

Groupes triviaux

Exemple - Avec l'addition

Exemple - Avec la multiplication

Ensemble $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Définition - Ensemble des classes d'équivalence modulo n
Soit $n \in \mathbb{N}$, fixé.
La relation $\equiv_n$ ou encore $\cdot \equiv \cdot [n]$ est une relation d'équivalence sur $\mathbb{Z}$.
L'ensemble des classes d'équivalence associées est noté $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.
Un système de représentant est $[[0, n-1]]]$, puisque $\dfrac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \dots \overline{n-1}\}$,
où pour tout $k \in [[0, n-1]]$, $\overline{k} = \{k, k+n, k+2n \dots k-n \dots\} = \{k + rn, r \in \mathbb{Z}\}$.
On peut alors définir sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ les lois $\overline{+}$ et $\overline{\times}$ par :

$$\overline{h}\overline{+}\overline{k} = \overline{h+k} \qquad \overline{h}\overline{\times}\overline{k} = \overline{h \times k}$$

Remarque - Le plus dur dans ce qui précède
est de démontrer que les lois $\overline{+}$ et $\overline{\times}$ sont bien définies.
C'est-à-dire qu'elles sont indépendantes des représentants de $\overline{k}$ et $\overline{h}$ choisis.
Nous ferons cette démonstration dans le cours d'arithmétique

Proposition - Groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{+}\right)$

Pour tout entier n, $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \overline{+}\right)$ est un groupe commutatif.

Son élément neutre est $\overline{0}$, et l'opposé de $\overline{k}$ est $\overline{n-k}$.

Démonstration

Analyse - Et pour la multiplication $\overline{\times}$?

Proposition - Groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}, \overline{\times}\right)$ avec p premier

Pour tout nombre premier p, $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}, \overline{\times}\right)$ est un groupe commutatif.

Son élément neutre est $\overline{1}$, et l'opposé de $\overline{p}$ est obtenu en exploitant le théorème de Bézout.

On peut donc obtenir l'inverse de $\overline{k}$ en exploitant l'algorithme d'Euclide.

Exercice

A démontrer

Remarque - Autre point de vue

Dans le cours sur les anneaux, nous définirons le groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}^{\star}, \overline{\times}\right)$, valable pour tout entier n, en ne considérant que les classes inversibles, modulo n.
Dans le cas où n est premier, on retrouve le groupe précédent.

« Petits » groupes

Comme les groupes sont réguliers, il ne peut y avoir chaque lettre ne peut apparaite plus d'une fois par ligne et par colonne.
Remplir ces tableaux, c'est comme remplir un carré latin (nom mathématique des sudoku).

Analyse - Groupe à deux éléments

Pour aller plus loin - Au début d'année...

Nous avons vu apparaître à plusieurs reprises des calculs avec $\{1, j, j^2\}$ (expression des racines d'un polynôme de degré 3 ou bien calcul de la somme $S_k = \sum_{i\equiv k[3]}^{n} \binom{n}{i}$...). Cela était nécessaire, car il s'agit de la meilleure incarnation du groupe (unique) à trois éléments

Pour aller plus loin - Groupes à 4 éléments

Il existe deux groupes à 4 éléments : $D_4 \simeq \{1, i, -1, -i\} \simeq \frac{\mathbb{Z}}{4\mathbb{Z}}$ et V_4 le groupe de Klein.

$V_4 :=$

$\top$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Il s'incarne par exemple dans le groupe des symétries par rapports aux médiatrices d'un triangle équilateral et de la transformation identité.

Exercice
Construire un (le) groupe de 3 éléments

Groupes matriciels

L'ensemble des matrices $(\mathcal{M}_{n,p}(\mathbb{K}),+)$ est un groupe. Il nous intéresse assez peu.
L'ensemble $(\mathcal{M}_n(\mathbb{K}),\times)$ n'est pas un groupe! (c'est un monoïde) Tous les éléments ne sont pas inversibles.
En revanche

— $(GL_n(\mathbb{K}),\times)$, ensemble des matrices inversibles est un groupe appelé, le groupe linéaire. Par définition : $GL_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) \mid \exists N \in \mathcal{M}_n(\mathbb{K})$ tel que $M \times N = N \times M = I_n\}$

— $(\mathcal{O}_n(\mathbb{K}),\times)$, ensemble des matrices orthogonales est un groupe appelé, le groupe orthogonal.
Par définition : $\mathcal{O}_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) \mid M^T \times M = I_n\}$

Groupes des permutations

Un groupe très important, on reviendra sur cette notion plus tard...

Proposition - Groupe des permutations d'un ensemble
Soit X un ensemble non vide. On note S_X l'ensemble des permutations de X (c'est-à-dire des bijections de X dans X). Alors $(S_X,\circ)$ est un groupe, généralement non commutatif, appelé groupe des permutations de X.

Remarque - Permutation
Qu'est-ce qu'une permutation de X ?
Il s'agit, par σ de changer « l'ordre » ou notre regard sur tous les éléments de X.
Donc cela signifie que

$$\{\sigma(x), x \in X\} = X$$

et donc σ est surjective. Il suffit de montrer que σ est injective : $\sigma(i) = \sigma(j) \Rightarrow i = j$..

Démonstration

Ce groupe non commutatif sera longuement étudié plus tard dans l'année.

Groupes et géométrie

Proposition - Groupes des similitudes directes du plan $\mathbb{C}$
L'ensemble des similitudes directes est un groupe pour la loi $\circ$.
L'élément neutre est l'identité.
L'inverse de la similitude de centre Ω, d'angle θ et de rapport k est la similitude de centre Ω, d'angle $-\theta$ et de rapport $\frac{1}{k}$.
L'inverse de la translation de vecteur $\vec{u}$ est la translation de vecteur $-\vec{u}$.

Pour aller plus loin - Programme d'Erlangen
Felix Klein (1849-1925) est un mathématicien allemand qui proposa dans le programme d'Erlangen de re« voir » toute les géométries en étudiant les groupes de symétrie qui agisse sur l'espace en question...
Il a eu une grosse influence sur Henri Poincaré.

Démonstration

4. Sous-groupe

4.1. Définition et caractérisations

Par la suite, on considérera $(G, \top)$ un groupe.

Définition - Sous-groupe
$H \subset G$ (non vide) est un sous-groupe de G si H est stable pour la loi interne et si la loi induite (restriction de la loi à H) munit H d'une structure de groupe. On note $H < G$

Proposition - Elément neutre et symétriques
Soit H un sous-groupe de G.
Alors l'élément neutre de H est l'élément neutre de G.
Si $x \in H$, le symétrique de x dans H est le symétrique de x dans G.

Démonstration

Théorème - Caractérisation 1
Soit $H \subset G$. H est un sous-groupe de G si et seulement si il vérifie :
— $H \neq \emptyset$
— $\forall (x, y) \in H^2,\ x \top y \in H$
— $\forall x \in H,\ x^{-1} \in H$

Pour aller plus loin - Le « monstre »
Il s'agit du plus gros groupe fini « connu ». On l'appelle le Monstre M ou groupe de Fischer-Griess F_1. Son ordre (= son cardinal ici) est $246 \times 320 \times 59 \times 76 \times 112 \times 133 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71 = 808017424794512875886459904961710757005754\,368\,000\,000\,000 \approx 8 \times 10^{53}$.
C'est bien un nombre fini (mais c'est gros). Il a été découvert (est-ce le bon verbe?) ou construit en 1980

Théorème - Caractérisation 2
Soit $H \subset G$. H est un sous-groupe de G si et seulement si il vérifie :
— $H \neq \emptyset$
— $\forall (x, y) \in H^2,\ x \top y^{-1} \in H$
(en notation multiplicative : $\forall (x, y) \in H^2,\ xy^{-1} \in H$;
en notation additive : $\forall (x, y) \in H^2,\ x - y \in H$)

Savoir faire - Démontrer que H est un (sous-)groupe
Dans la pratique, lorsque H est une partie de E, groupe. On démontre qu'il s'agit d'un sous-groupe de E
— avec la caractérisation 1, lorsque H et E sont explicites
— avec la caractérisation 2, lorsque H et E sont théoriques

Pour aller plus loin - Action de groupe et représentation
Étant donné un groupe G, dont la loi est notée multiplicativement et dont l'élément neutre est noté e, on peut définir une action (ou opération) de G sur un ensemble E par une application : $G \times E \to E$, $(g, x) \mapsto g \cdot x$ vérifiant les propriétés suivantes : $\forall\, x \in E$, $e \cdot x = x$ et $\forall\, g, g' \in G$, $\forall\, x \in E$, $g' \cdot (g \cdot x) = (g \top g') \cdot e$.
De (très) nombreuses situations de présence de groupe sont de cette forme là, avec un ensemble E donné.
Réciproquement, si on connait très bien E sur lequel agit G, alors on apprend à connaître G.
La notion d'orbite, de permutations de E, d'action fidèle... permettent de mieux cerner « notre objet ».

Démonstration

Exercice
Montrer que si $H_1 < (G_1, \perp)$ et $H_2 < (G_2, \top)$ alors $H_1 \times H_2$ est un sous-groupe du groupe produit $(G_1 \times G_2, \star)$.

4.2. Intersection

Théorème - Intersection de deux sous-groupes
Soit H et K deux sous-groupes de $(G, \top)$.
Alors $H \cap K$ est un sous-groupe de G.

Démonstration

L'exercice suivant donne TOUS les sous-groupes de $(\mathbb{Z}, +)$:
Exercice

1. Soit $a \in \mathbb{Z}$. Montrer que $a\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.
2. Soit G un sous-groupe de $(\mathbb{Z}, +)$, $G \neq \{0\}$.
   Justifier que $G \cap \mathbb{N}^*$ a un plus petit élément $a > 0$.
   Montrer que $G = a\mathbb{Z}$ (utiliser la division euclidienne).

La démonstration s'adpate à une infinité de sous-groupe.

Théorème - Intersection de sous-groupes
Soit $(H_i)_{i \in I}$ une famille de sous-groupes de $(G, \top)$. Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

Démonstration

4.3. Sous-groupe engendré

Première manipulation (trouver un candidat)

Analyse - Plus petit groupe contenant une partie A de G

Définition - Groupe engendré
Soit $(G,\top)$ un groupe. Soit A une partie de G.
On appelle groupe engendré par A, le plus petit sous-groupe de G, parmi les sous-groupes de G contenant A.
On le note $< A >$. On a donc $< A >= \bigcap_{H\in\mathscr{A}} H = \min \mathscr{A}$
(où $\mathscr{A} = \{H < G \mid A \subset H\}$).

Il faut démontrer que $\bigcap_{H\in\mathscr{A}} H$ est bien le plus petit sous-groupe de G contenant A.

Démonstration

Proposition - Croissance de l'engendrement
Si $A \subset B$ sont deux parties d'un groupe G.
Alors $< A > \subset < B >$

Démonstration

Application - Réflexes

Savoir faire - Comment trouver le sous-groupe engendré par une partie A?

Il faut

1. *Pré-sentir* la bonne description (efficace) de ce sous-groupe.
   On donne alors un nom à cet ensemble K.
2. Montrer que K est bien un groupe, qui contient A
3. Montrer que K est nécessairement entièrement inclus dans $< A >$ ou dans tout sous-groupe de $\mathscr{A}$.

Comme $< A >$ est le plus petit sous-groupe contenant A, propriété vérifiée par K, alors $< A >= K$

Croissance par engendrement (deuxième point de vue)

Attention - Nom contradictoire?

Ce nom semble contradictoire. Par groupe engendré on entend plutôt quelque chose qui s'agrandit (pour l'inclusion) à partir de A, alors qu'il s'agit visiblement de quelque chose qui diminue à partir de G.
A-t-on la même chose?

Analyse - Engendrement

Exemple - Groupes engendré par p dans $\mathbb{Z}$.

Exercice

Quel est le sous-groupe engendré par $\{p, q\}$ dans $(\mathbb{Z}, +)$?

Groupe monogène

Définition - Groupe monogène
On dit que G est un groupe monogène, s'il existe $x \in G$ tel que $G =< x >$.
Dans ce cas $G = \{x^k, k \in \mathbb{Z}\}$.

Savoir faire - Etudier des groupes monogènes
Si G est un groupe que l'on sait monogène, alors il existe $x \in G$ (référence, que l'on fixe) tel que $G =< x >$.
L'application $\varphi : \mathbb{Z} \to G$, $k \mapsto x^k$ est bien définie, surjective. Elle peut être injective ou non (cas fini).
On transfère ensuite par φ (ou φ^{-1}) l'étude de G, à partir de propriétés de $\mathbb{Z}$.

Exercice
Montrer qu'un groupe monogène est nécessairement abélien

Pour aller plus loin - De qui parle Felix Klein?
« Depuis longtemps déjà, il s'occupait à étudier des groupements de racines complexes de l'unité sur la base de sa théorie des racines primitives. Et voilà que ce matin-là (le 30 mars 1796) en se réveillant, il lui apparut clairement qu'à partir de sa théorie, on pouvait construire un polygone à 17 cotés[...]. Cet événement marqua un grand tournant dans sa vie : c'est précisément ce jour-là qu'il décida d'abandonner les langues pour se consacrer exclusivement aux mathématiques ». Les mathématiques y ont beaucoup gagné!

Exemples à partir de $\mathbb{U}$

L'exercice suivant nous aide à faire le point.
Exercice
On considère le groupe $(\mathbb{U}, \times)$.

1. Soit $z_k = e^{\frac{2i\pi}{k}}$. Que vaut le groupe $< z_k >$?
2. Avec les mêmes notations, que vaut le groupe $< z_r, z_s >$?
3. A-t-on pour tout $n \in \mathbb{N}$, pour tout $z \in \mathbb{U}_n$, $\mathbb{U}_n =< z >$?
   Sinon, à quelle condition sur z, a-t-on : $\mathbb{U}_n =< z >$?
4. Quel est le groupe $\mathbb{U}_n \cap \mathbb{U}_m$?
5. $\mathbb{U}$ est-il monogène ?

4.4. Démontage d'un groupe

Théorème de Lagrange

Proposition - Relation d'équivalence modulo un sous-groupe
Soit $(G, *)$ un groupe et $H < G$, un sous-groupe de G.
On note $\mathscr{R}_H$, la relation définie sur G par :

$$a \mathscr{R}_H a' \Longleftrightarrow a^{-1} * a' \in H$$

Alors $\mathscr{R}_H$ est une relation d'équivalence.

Démonstration

Remarque - Lien relation d'équivalence et sous-groupe
On voit sur cette démonstration le lien très étroit qui unit les caractéristiques d'un sous-groupe et les propriétés d'une relation d'équivalence. Plus précisément : l'élément neutre à la réflexivité, l'inversibilité à la symétrie et la stabilité à la transitivité   Quand on a une relation d'équivalence, on a naturellement une décomposition en réunion disjointe

Proposition - Décomposition de G
Soit H un sous-groupe de G.
On note $S := S_{\frac{G}{\mathscr{R}_H}}$ un système de représentant des classes d'équivalences de $\mathscr{R}_H$.
Alors $G = \biguplus_{a\in S}\overline{a}$, la réunion disjointes des classes de a.
$\overline{a}$ n'est pas un groupe, mais il est en bijection avec H.
Par la suite, on notera aH, cet ensemble. On a donc $aH = a'H \Leftrightarrow a\mathscr{R}_H a' \Leftrightarrow a^{-1}a' \in H$
Le produit cartésien $H \times S$ et le groupe G sont en bijection (c'est la décomposition).

Démonstration

En fait, les ensembles $\overline{a}$ sont comme des sous-groupes affines de G...

Proposition - Théorème de LAGRANGE
Si H un sous-groupe de G, groupe de cardinal fini, alors $\text{card}H|\text{card}G$.

Démonstration

Sous-groupe distingué

Analyse - S comme un groupe?

Définition - Sous-groupe distingué
On dit que $H < G$ est un sous-groupe distingué (ou normal) de G si

$$\forall\ a \in G, \forall\ x \in H, \qquad a^{-1}xa \in H$$

On peut retenir que pour tout $a \in G$, $aH = Ha$.
On note alors $H \triangleleft G$

Démonstration

Proposition - Groupe quotient
Soit $(G, *)$ un groupe.
Si $H \triangleleft G$ est un sous-groupe distingué de G, alors $S = \dfrac{G}{\mathscr{R}_H}$, souvent noté $\dfrac{G}{H}$ est un groupe pour la loi $\overline{*}$ définie par $aH \overline{*} bH = (a * b)H$.

Exercice
A démontrer ! (Attention, ce n'est pas un sous-groupe. Il faut donc tout redémontrer à commencer par la bonne définition de la loi. . .)

Exemple - Groupe trivial

Exemple - G abélien

Définition - Groupe simple
On dit qu'un groupe est simple lorsqu'il ne possède pas de sous-groupe distingué autre que $\{e\}$ et lui-même

Pour aller plus loin - Théorie de résolution par radicaux
Comme écrit wikipédia : « Pour n supérieur ou égal à 5, le groupe alterné sur n éléments $\mathscr{A}_n$ est simple. Ce résultat est à la base de la théorie de la résolution par radicaux. »

Cela ne vous rappelle pas une autre définition ?

Exercice
Soit G un groupe de cardinal p, premier.
Montrer que G est simple

5. Morphismes de groupes

5.1. Définition et propriété immédiate

Soient $(G,\star)$ et $(G',\top)$ deux groupes.

Définition - Morphisme de groupes
Une application f de G dans G' vérifiant :
$$\forall (x,y)\in G^2,\ f(x\star y)=f(x)\top f(y).$$
est appelé morphisme (de groupes) de $(G,\star)$ sur $(G',\top)$.

Proposition - Conservation du noyau
Soit $f : G \to G'$ un morphisme de groupes. Alors $f(e_G)=e_{G'}$.

Démonstration

Proposition - Image de l'inverse
Soit $f : G \to G'$ un morphisme de groupes.
Alors pour tout $x\in G$, $f(x^{-1})=\left(f(x)\right)^{-1}$

Démonstration

Exemple - exp

5.2. Image et noyau d'un morphisme

> **Proposition - Sous-groupe**
> Soit $f : G \to G'$ un morphisme de groupes.
> Soit A un sous-groupe de G, alors $f(A)$ est un sous-groupe de G'.
> Soit B un sous-groupe de G', alors $f^{-1}(B)$ est un sous-groupe de G.
> En particulier :
> - $\operatorname{Im} f = f(G) = \{f(x), x \in G\}$ est un sous-groupe de G', appelé image de G
> - $\operatorname{Ker} f = f^{-1}(e_{G'}) = \{x \in G \mid f(x) = e_{G'}\}$ est un sous-groupe de G, appelé noyau de f.

Exemple - $\mathbb{Z} \to \mathbb{U}_n$

Démonstration

<u>Exercice</u>
Montrer que $f : G \to G'$ morphisme de groupes est :
- surjective ssi $\operatorname{Im} f = G'$
- injective ssi $\operatorname{Ker} f = \{e_G\}$

Exemple - $\operatorname{Ker} f$ **est un sous-groupe distingué**

5.3. Premier théorème d'isomorphisme

Théorème - Premier théorème
Soient G et G' deux groupes et $f : G \to G'$, un morphisme de groupes.
Alors f induit un isomorphisme de groupes : $\hat{f} : G/\text{Ker}\, f \hookrightarrow\!\!\!\!\rightarrow \text{Im}\, f$.

Démonstration

Pour aller plus loin - Une deuxième, un troisième ?
Le deuxième énonce :
si $N \lhd G$ et $H < G$, alors $N \cap H \lhd H$ et $H/(N \cap H) \hookrightarrow\!\!\!\!\rightarrow HN/N$.
Le troisième énonce :
si $N, M \lhd G$ tels que $M < N$, alors $N/M \lhd G/M$ et $(G/M)/(N/M) \hookrightarrow\!\!\!\!\rightarrow G/N$.

Remarque - Notation symbolique ou formelle
On retrouve dans la littérature (mathématique) le diagramme suivant que l'on qualifie de commutatif :

$$G \twoheadrightarrow \frac{G}{\text{Ker}\, f} \hookrightarrow\!\!\!\!\rightarrow \text{Im}\, f \hookrightarrow G'$$

6. Bilan

Pour aller plus loin - Dans les espaces vectoriels...
Ce théorème est à comparer avec le lemme préparatoire qui conduit au si fondamental théorème du rang dans les espaces vectoriels de dimension finie.
Ainsi si f est une application linéaire de E sur F, avec E de dimension finie.
Alors $\dim E = \dim Im\, f + \dim \text{Ker}\, f$ car $f_{|H} : H \to Im\, f$ est une application bijective (où H tel que $E = H \oplus Ker\, f$.

Synthèse

- ⇝ La notion de groupe est la brique élémentaire des théories mathématique. C'est une notion primitive : un ensemble et une loi interne associative, unifère et dont tous les éléments sont symétriques. Cette structure est naturellement comparable à une relation d'équivalence : associativité↔ transitivité, élément neutre↔reflexivité et inversion↔symétrie.
- ⇝ On peut réduire des (sous-)groupes par intersection, ou bien générer des (sous-)groupes par engendrement de parties. Ces deux méthodes sont très classiques en algèbre ou en topologie.
- ⇝ On décompose ensuite les groupes en produit de sous-groupes à condition que le premier de ce produit soit un sous-groupe distingué. Finalement les sous-groupes distingués (ou normaux) sont comme des nombres premiers.
- ⇝ On peut aussi déplacer des structures avec des morphismes de groupes, voire comparer des groupes (est-ce que ces morphismes sont bijectives (isomorphisme) ?)

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Démontrer que H est un (sous-)groupe
— Savoir-faire - Comment trouver le sous-groupe engendré par une partie A ?
— Savoir-faire - Etudier des groupes monogènes

Notations

Notations	*Définitions*	*Propriétés*	*Re*
$H < G$	H est un sous-groupe de G	$e_G \in H$ et $\forall\ x, y \in H,\ xy^{-1} \in H$	Pa
$H \lhd G$	H est sous-groupe distingué de G	$H \lhd G$ et $\forall\ x \in G,\ xHx^{-1} \subset H$	Pa
$\frac{G}{H}$	Ensemble des classes d'équivalence sur G pour la relation d'équivalence $a\mathscr{R}_H b \iff ab^{-1} \in H$	Les classes d'équivalence sont chacune en bijection avec H.	On GR

Retour sur les problèmes

59. Groupes, anneaux, corps...
60. Pas facile. Il faut plonger dans un cours sur le corps de Galois. Lorsqu'on aura fait le cours sur le groupe symétrique (= groupe des permutations d'un ensemble à n éléments), cela sera peut-être plus simple...
    En gros une formule de résolution, c'est une décomposition du groupe des permutations (qui agit sur l'ensemble des racines) en sous-groupe distingué × groupe quotient. Si une telle décomposition n'est pas possible (le groupe est simple), nous sommes bloqués. Or pour les équations de degré 5, on regarde S_5 (cf second semestre), il se décompose en $A_5 t \times \{-1, 1\}$, mais A_5 ne se décompose pas plus...
61. La composition conserve nécessairement la distance.
    La question fondamentale est dans l'existence de la transformation inverse (bijectivité de φ).
    A noter qu'il s'agit d'un groupe continue (ou de LIE) par opposition aux groupes discrets (et souvent finis comme S_n).