Groupes

Contents

1 Groupes et sous-groupes

1.1 Groupes

1.1.1 Définition

Soit G un ensemble muni d'une loi de composition notée . $(G, .)$ est un groupe si :

1) la loi est associative
2) il existe un élément neutre e
3) tout élément possède un symétrique

Simplifier

Dans un groupe, on peut simplifier :

$$x.y = x.z \Rightarrow y = z$$

Inverse d'un produit

Dans un groupe G :

$$\forall x, y \in G, (x.y)^{-1} = y^{-1}.x^{-1}$$

1.1.2 Premiers exemples

Loi notée $+$: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$...
Loi notée $\times$: $\mathbb{R}^*$, $\mathbb{U}$, $\{-1, 1\}$...
Loi notée $\circ$: S_n.

1.1.3 Unicité de l'élément neutre

$$e_1.e_2 = e_1 = e_2$$

1.1.4 Equation $x^2 = x$

Dans un groupe G, l'élément neutre est le seul à vérifier $x^2 = x$.

Démonstration

Si $x^2 = x$, alors $x^{-1}.x^2 = x^{-1}.x = e$, d'où $x = e$.

Remarque

Comment expliquer que dans $(L(E), \circ)$ ce soit différent ?

1.1.5 Equation $x.y = e$

Dans un groupe G, si $x.y = e$, alors y est l'inverse de x.

Démonstration

Si $x.y = e$, alors $x^{-1}.(x.y) = x^{-1}$, d'où $\left(x^{-1}.x\right).y = x^{-1}$.
Finalement

$$y = x^{-1}$$

Remarque

$x.y = e$ ne prouve pas que y est l'inverse de x si on ne sait pas que G est un groupe ; il faut montrer que

$$x.y = y.x = e$$

1.1.6 Le groupe $\mathbb{U}_n$

$\mathbb{U}_n = \{z \in \mathbb{C} / z^n = 1\}$. Egalement : $\mathbb{U}_n = \left\{\omega^k / 0 \leq k \leq n-1\right\}$ avec $\omega = ?$

Réponse

$$\omega = \exp\left(\frac{2i\pi}{n}\right)$$

1.1.7 Les translations

Soit a un élément d'un groupe G ; soit

$$\begin{array}{rccc} t_a : & G & \to & G \\ & x & \to & a.x \end{array}$$

t_a est une bijection, d'inverse ?

Réponse

$$t_a \circ t_{a^{-1}} = t_{a^{-1}} \circ t_a = \mathrm{Id}_G$$

Donc t_a est une bijection.

De même : $x \to x.a$ est une bijection de G sur G. Encore une : $x \to x^{-1}$.

Cas particulier important

Soit $a \in G$ et H un sous-groupe de G ; on note :

$$aH = \{ah / h \in H\} = t_a(H)$$

et

$$Ha = \{ha / h \in H\}$$

Si H est fini, aH et Ha ont le même cardinal que H.

1.2 S_n

S_n est le groupe des permutations de $\{1, ..., n\}$; son cardinal est $n!$.

Définition

Le support d'une permutation $\sigma \in S_n$ est

$$\{x \in [\![1, n]\!] / \sigma(x) \neq x\}$$

Cycles

Pour $p \geq 2$, on note $c = (a_1\ a_2\ ...\ a_p)$ la permutation définie par
$\mathrm{c}(a_j) = a_{j+1}$ si $1 \leq j \leq p-1$
$c(a_p) = a_1$
$c(x) = x$ sinon.
Le support de c est donc $\{a_1, ..., a_p\}$.

Théorème

Tout élément de S_n est produit de cycles à supports disjoints.

1.3 Produit de deux groupes

1.3.1 Définition

Soit G_1 et G_2 deux groupes ; on définit une loi de composition interne sur $G = G_1 \times G_2$ de la manière suivante :

$$(x_1, x_2).(y_1, y_2) = (x_1.y_1, x_2.y_2)$$

On vérifie que G est un groupe pour cette loi.

1.3.2 Exemples

$\mathbb{R}^2$, $\mathbb{R}^3$...

1.3.3 Généralisation

On généralise aisément au produit d'un nombre fini de groupes.

1.4 Sous-groupe

1.4.1 Loi induite

Soit A une partie d'un groupe $(G,.)$; on dit que A est stable si :

$$\forall x, y \in A,\ x.y \in A$$

Dans ce cas, on peut définir une loi sur A, appelée loi induite.

1.4.2 Sous-groupe

On dit que H est un sous-groupe de $(G,.)$ si H est stable et si H est un groupe pour la loi induite.

Caractérisation

H est un sous-groupe de $(G,.)$ si
- $H \subset G$
- H contient e_G
- H est stable
- $\forall x \in H,\ x^{-1} \in H$

1.4.3 Remarque

Soit H est un sous-groupe de $(G,.)$; soit x et y deux éléments de G ; que dire de $x.y$
- si les deux sont dans H ?
- un seul des deux ?
- aucun des deux ?

1.5 Sous-groupe engendré par une partie

1.5.1 Théorème

L'intersection H de toute famille $(H_i)_{i\in I}$ de sous-groupes de G en est un.
On ne suppose pas que I est fini.

Démonstration

- $\forall i \in I,\ e \in H_i$; donc $e \in H$.
- Soit x et y deux éléments de H : $\forall i \in I,\ x \in H_i$ et $\forall i \in I,\ y \in H_i$.
  Les H_i étant des sous-groupes :

$$\forall i \in I,\ x.y \in H_i$$

  Donc

$$x.y \in H$$

- Soit x un élément de H : $\forall i \in I,\ x \in H_i$.
  Les H_i étant des sous-groupes :

$$\forall i \in I,\ x^{-1} \in H_i$$

  Donc :

$$x^{-1} \in H$$

1.5.2 Exercice

On suppose que le groupe G est l'union de deux sous-groupes :

$$G = H \cup K$$

Montrer que...

1.5.3 Sous-groupe engendré par une partie

Soit A une partie d'un groupe $(G, .)$; l'ensemble des sous-groupes de G contenant A possède un plus petit élément $\langle A \rangle$; on l'appelle sous-groupe de G engendré par A.

Démonstration

Soit H l'intersection des sous-groupes de G contenant A.
- H est un sous-groupe de G.
- H contient A.
- Soit H' un sous-groupe de G contenant A ; $H \subset H'$, pourquoi ?

Analogie

Enveloppe convexe, sous-espace vectoriel engendré,...

1.5.4 Caractérisation

On suppose A non vide ; dans ce cas, $\langle A \rangle$ est l'ensemble des produits finis des éléments de A et de leurs inverses.

Démonstration

Soit H l'ensemble des produits des éléments de A et de leurs inverses.
Plus précisément :

$$H = \bigcup_{n \geq 1} H_n$$

avec

$$H_n = \left\{ x_1.x_2...x_n / \, x_1, ..., x_n \in A \cup A^{-1} \right\}$$

- H est un sous-groupe de G.
- H contient A.
- Soit H' un sous-groupe de G contenant A ; $H \subset H'$, pourquoi ?

Conclusion :

$$H = \langle A \rangle$$

1.5.5 Un cas particulier

Si $A = \{a\}$:

$$\langle a \rangle = \left\{ a^k / k \in \mathbb{Z} \right\}$$

Un groupe engendré par un singleton est appelé monogène.

Remarque

Ce sous-groupe est abélien.

Remarque

Si la loi est notée $+$:

$$\langle a \rangle = \{ k.a / k \in \mathbb{Z} \}$$

Exemples

$\mathbb{Z}$, $\mathbb{U}_n$.

1.6 Sous-groupes de $\mathbb{Z}$

Les sous-groupes de $(\mathbb{Z},+)$ sont les $a\mathbb{Z}$, où a décrit $\mathbb{N}$.

Démonstration

$a\mathbb{Z}$ est l'image d'un morphisme de groupes

Lequel ?

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ k & \to & k.a \end{array}$$

Réciproquement : soit H un sous-groupe de $(\mathbb{Z},+)$ non réduit à $\{0\}$.

On pose $a = ...$?

Réponse

$$a = \min H \cap \mathbb{N}^*$$

Il est clair que $a\mathbb{Z} \subset H$.

Soit x un élément de H ; on écrit

$$x = aq + r$$

avec $0 \leq r \leq a-1$.

On constate que

$$r = x - aq \in H \cap [\![0, a-1]\!]$$

Donc $r = 0$ et $x \in a\mathbb{Z}$. Conclusion :

$$H = a\mathbb{Z}$$

1.7 Inversibles d'un monoïde

Exercice

Soit E un ensemble muni d'une loi de composition interne associative et possèdant un élément neutre.

Dans ce cas, l'ensemble G des éléments inversibles de E constitue un groupe.

1.8 $x^2 = e_G$

Exercice

Soit G un groupe tel que

$$\forall x \in G, x^2 = e$$

Montrer que G est abélien.

Démonstration

$$\forall x, y \in G,\ x.y = (x.y)^{-1} = y^{-1}.x^{-1} = y.x$$

Remarque : si de plus G est fini, on peut montrer que son cardinal est une puissance de deux.

2 Morphismes de groupes

2.1 Définition

Soit G_1 et G_2 deux groupes ; f est un morphisme de groupes de G_1 dans G_2 si :

$$\forall x, y \in G_1, f(x.y) = f(x).f(y)$$

Autrement dit, l'image d'un produit est le produit des images.

On dit aussi endomorphisme si $G_1 = G_2$.

2.2 Premiers exemples

2.2.1 De $\mathbb{R}$ dans $\mathbb{R}_+^*$

2.2.2 De $\mathbb{C}^*$ dans $\mathbb{R}_+^*$

2.2.3 De $GL_n(K)$ dans K^*

2.2.4 De S_n dans $\mathbb{C}^*$

2.3 Propriétés

2.3.1 Image de l'élément neutre

Si f est un morphisme de groupes de G_1 dans G_2, alors

$$f(e_1) = e_2$$

Démonstration

Soit $a = f(e_1)$; $e_1.e_1 = e_1$, d'où

$$a = f(e_1) = f(e_1.e_1) = a.a$$

Or, on sait que dans un groupe, l'élément neutre est la seule solution de l'équation $a^2 = a$.

2.3.2 Image d'un inverse

L'image d'un inverse par un morphisme de groupes est l'inverse de l'image.

Démonstration

Soit y l'inverse de x : $x.y = e_1$; alors

$$f(x).f(y) = f(x.y) = f(e_1) = e_2$$

Donc

$$f\left(x^{-1}\right) = (f(x))^{-1}$$

Remarque

Si les deux lois sont notées $+$:

$$f(-x) = -f(x)$$

2.3.3 Endomorphismes de $\mathbb{Z}$

Exercice

Les endomorphismes de $(\mathbb{Z}, +)$ sont les

$$f_a : k \to a.k$$

où a décrit $\mathbb{Z}$.

2.4 La signature

2.4.1 Théorème

Soit $n \geq 1$. Il existe un unique morphisme de groupes ε de S_n dans $\mathbb{U}_2$ tel que, pour toute transposition t, $\varepsilon(t) = -1$. On l'appelle la signature.

2.4.2 Signature d'un cycle

Si $\sigma = (a_1\ a_2\ ...\ a_p)$:

$$\varepsilon(\sigma) = (-1)^{p-1}$$

En effet :

$$\sigma = (a_1\ a_2\ ...\ a_p) = (a_1\ a_2) \circ ... \circ (a_{p-1}\ a_p)$$

2.4.3 Cas général

La signature d'une permutation σ est

$$(-1)^{n-\lambda}$$

où λ est le nombre d'orbites, y compris les orbites réduites à un singleton.

Se ramène au cas précédent en décomposant σ en produit de cycles à supports disjoints.

2.5 Image

Théorème

L'image, l'image réciproque d'un sous-groupe par un morphisme de groupes est un sous-groupe.

Cas particulier

$f(e_1) = e_2$ si f est un morphisme de groupes de G_1 dans G_2.

Il s'agit d'une propriété, et non d'un axiome.

2.6 Noyau

Notons $K = \ker f$ l'image réciproque de $\{e_2\}$.

2.6.1 Antécédents d'un élément

Soit $b \in G_2$; supposons que b possède au moins un antécédent a par f : $f(a) = b$.

Cherchons les autres antécédents de b :

$$\forall x \in G_1, f(a) = f(x) \iff f(a)^{-1}.f(x) = e_2 \iff f\left(a^{-1}.x\right) = e_2 \iff a^{-1}.x \in K$$

D'où :

$$\forall x \in G_1, f(a) = f(x) \iff x \in aK$$

On constate que l'ensemble des antécédents de b est aK :

$$f^{-1}(\{b\}) = aK$$

En particulier, si K est fini, b a le même nombre d'antécédents que e_2.

En notation additive

$$f^{-1}(\{b\}) = a + \ker f$$

C'est en particulier le cas pour les applications linéaires.

2.6.2 Théorème

f est injectif si et seulement si $\ker f = \{e_1\}$.

Démonstration

Découle facilement de ce qui précède.

2.6.3 $\mathbb{U}_n$

$\mathbb{U}_n$ est le noyau d'un morphisme de groupes ; lequel ?

Réponse

$z \to z^n$, de $\mathbb{C}^*$ dans $\mathbb{C}^*$.

2.6.4 $SL_n(K)$

$SL_n(K)$ est le noyau d'un morphisme de groupes ; lequel ?

Réponse

$M \to \det M$, de $GL_n(K)$ dans K^*.

2.6.5 $SO(n)$

$SO(n)$ est le noyau d'un morphisme de groupes ; lequel ?

Réponse

$M \to \det M$, de $O(n)$ dans $\mathbb{R}^*$.

2.7 Isomorphismes

2.7.1 Définition

On appelle isomorphisme un morphisme de groupes de G_1 dans G_2 bijectif .
On dit aussi automorphisme si de plus $G_1 = G_2$.

2.7.2 Théorème

Si f est un isomorphisme de G_1 dans G_2, f^{-1} est un isomorphisme de G_2 dans G_1.

Démonstration

Notons $g = f^{-1}$; soit x_2, y_2 deux éléments de G_2 ; soit x_1, y_1 leurs antécédents par f ; on part de

$$f(x_1.y_1) = f(x_1).f(y_1) = x_2.y_2$$

On compose par $g = f^{-1}$:

$$x_1.y_1 = g(x_2.y_2)$$

Finalement :

$$g(x_2).g(y_2) = g(x_2.y_2)$$

2.7.3 Automorphismes de $(\mathbb{Z}, +)$

Exercice

Trouver les automorphismes de $(\mathbb{Z}, +)$.

Réponse

Id et $-$Id.

2.7.4 Un exemple de produit

Exercice

Montrer que $\mathbb{C}^*$ est isomorphe à un produit de deux groupes.

Réponse

$$\begin{array}{c} f :]0, +\infty[\times \mathbb{U} \to \mathbb{C}^* \\ (r, u) \to r.u \end{array}$$

2.7.5 Automorphismes intérieurs

Exercice

Soit a élément d'un groupe G, et

$$f : x \to a.x.a^{-1}$$

On vérifie aisément que f est un automorphisme de groupe, appelé intérieur.

2.8 $|G| = |\ker f| \,.\, |\mathrm{Im} f|$

Exercice

Soit G un groupe fini, et f un morphisme de groupes de G dans G' ; alors

$$|G| = |\ker f| \,.\, |\mathrm{Im} f|$$

Démonstration

On a vu que les éléments de $\mathrm{Im} f$ ont tous le même nombre d'antécédents.
On notera $K = \ker f$, $\mathrm{Im} f = \{b_1, ..., b_n\}$ et

$$A_j = f^{-1}(b_j)$$

La famille $(A_j)_{1 \leq j \leq n}$ est une partition de G ; les A_j ont tous le même cardinal que K ; donc

$$|G| = n.\,|K| = |\ker f| \,.\, |\mathrm{Im} f|$$

3 Groupe $\mathbb{Z}/n\mathbb{Z}$

$n \in \mathbb{N}^*$ est fixé.

3.1 Congruence

On note $x \equiv y\,[n]$ si n divise $y - x$; on vérifie qu'il s'agit d'une relation d'équivalence dans $\mathbb{Z}$.

Remarque

$$\forall x, y \in \mathbb{Z},\ x \equiv y\,[n] \Leftrightarrow y - x \in n\mathbb{Z}$$

Les trois axiomes d'une relation d'équivalence se démontrent en utilisant les trois propriétés de sous-groupe de $n\mathbb{Z}$.

3.2 Classes d'équivalence

Notation $\overline{a}$:

$$\overline{a} = a + n\mathbb{Z}$$

Remarque

$\overline{a}$ contient un seul élément qui est aussi dans $[0, n-1]$.

3.3 Définition de $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence ; exemples : $n = 2$, $n = 3$.
D'après la remarque précédente :

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\}$$

3.4 L'addition dans $\mathbb{Z}/n\mathbb{Z}$

On se propose de définir une addition dans $\mathbb{Z}/n\mathbb{Z}$; il est naturel de procéder ainsi :

Soit $\alpha = \overline{a}$ et $\beta = \overline{b}$; on pose

$$\alpha + \beta = \overline{a+b}$$

Un exemple :

$n = 100$; $\alpha = \overline{125}$; $\beta = \overline{28}$; on pose $\alpha + \beta = \overline{125+28}$.

Problème :

il y a plusieurs représentants dans chaque classe ; combien ? Il est donc nécessaire de vérifier que le résultat $\alpha + \beta$ ne dépend que de α et β.

3.4.1 Lemme

Si $a' \equiv a\,[n]$ et $b' \equiv b\,[n]$, alors

$$a' + b' \equiv a + b\,[n]$$

Démonstration

Supposons $a' = a + np$ et $b' = b + nq$ avec $p, q \in \mathbb{Z}$; alors :

$$a' + b' = (a+b) + n\,(p+q)$$

et donc

$$a' + b' \equiv a + b\,[n]$$

3.4.2 Théorème

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.

Elément neutre

C'est $e = \overline{0} = \overline{n} = n\mathbb{Z}$.

Opposés

L'opposé de $\overline{k}$ est $\overline{-k}$; en effet :

$$\overline{k} + \overline{-k} = \overline{k-k} = \overline{0}$$

3.5 Générateurs

3.5.1 Remarque

$\overline{1}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$.

3.5.2 Théorème

$\alpha = \overline{a}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$.

Démonstration

Le sous-groupe H de $\mathbb{Z}/n\mathbb{Z}$ engendré par α est $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\overline{1} \in H$; ce qui équivaut à :

$$\exists k \in \mathbb{Z}, \overline{1} = k.\overline{a}$$

ou a

$$\exists k \in \mathbb{Z}, \exists q \in \mathbb{Z},\ 1 = ka + nq$$

On conclut à l'aide du théorème de Bézout.

3.5.3 Exemple

$n = 15$; $a = 4$; $\alpha = \overline{4}$; $2\alpha = \overline{8}$; $3\alpha = \overline{12}$; $4\alpha = \overline{1}$; $5\alpha = \overline{5}$...

4 Ordre d'un élément dans un groupe

4.1 Un morphisme

Soit a un élément d'un groupe G ; on définit un morphisme φ_a ainsi :

$$\varphi_a : \begin{array}{c} \mathbb{Z} \to G \\ k \to a^k \end{array}$$

φ_a est bien un morphisme de groupes ; son image est $\langle a \rangle$, le sous-groupe de G engendré par a ; son noyau est un sous-groupe de $\mathbb{Z}$.

4.2 1er cas

φ_a est injectif, ce qui signifie que :

$$\forall k \in \mathbb{Z} - \{0\}, a^k \neq e_G$$

Dans ce cas, $\langle a \rangle$ est isomorphe à $\mathbb{Z}$; on dit que a est d'ordre infini.

Exemples dans $\mathbb{Z}$, $\mathbb{R}^*$, $\mathbb{C}^*$, $GL_n(\mathbb{C})$ ...

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

4.3 2e cas

φ_a n'est pas injectif ; $\ker \varphi_a = n\mathbb{Z}$ avec $n \geq 1$; n est appelé l'ordre de a ; remarquons que

$$n = \min \left\{ k \geq 1 / a^k = e_G \right\}$$

Dans ce cas, la suite $\left(a^k\right)_{k \in \mathbb{Z}}$ est périodique, de période n.

4.3.1 Exemples dans $\mathbb{C}^*$

$a = 1, -1, i, j, \exp\left(\frac{2i\pi}{n}\right)$.

4.3.2 Exemple dans S_n

$c = (a_1\, a_2 \ldots a_p)$.

4.3.3 Image de φ_a

Le sous-groupe engendré par a est de cardinal n :

$$\langle a \rangle = \left\{ e, a, a^2, ..., a^{n-1} \right\}$$

4.3.4 Un isomorphisme

φ_a induit un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur $Gr(a)$: $\overline{k} \to a^k$, qui est bien défini...

Démonstration

Supposons $\alpha = \overline{p} = \overline{q}$; alors $q - p \in n\mathbb{Z} = \ker\varphi_a$; donc $\varphi_a(p) = \varphi_a(q)$; d'où

$$a^p = a^q$$

En particulier, l'ordre de a est le cardinal du sous-groupe engendré par a.

4.4 Synthèse

Définition

Un groupe monogène fini est appelé groupe cyclique.

Théorème

Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$.

Tout groupe cyclique de cardinal n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Deux groupes cycliques de même cardinal sont donc isomorphes.

L'ordre d'un élément

Soit a un élément d'un groupe G et $k \in \mathbb{Z}$.

$a^k = e_G$ si et seulement si l'ordre de a divise k.

Le sous-groupe engendré par a

Soit a un élément d'un groupe G.

Si n est l'ordre de a, le sous-groupe de G engendré par a est un sous-groupe de G de cardinal n.

4.5 L'ordre divise le cardinal

La démonstration n'est exigible que pour G commutatif

4.5.1 Théorème

Soit a un élément d'un groupe G de cardinal n ; alors

$$a^n = e$$

Autrement dit, l'ordre de a divise n.

4.5.2 Démonstration si G est abélien

$G = \{g_1, ..., g_n\}$; soit p le produit des éléments de G :

$$p = g_1 ... g_n$$

Soit $t : x \to a.x$; étudions

$$q = \prod_{j=1}^{n} t\left(g_j\right) = \prod_{j=1}^{n} \left(a.g_j\right) = a^n.p$$

car G est abélien

Par ailleurs, $p = q$ car t est une permutation de G et G abélien.
Conclusion ?

$$p = a^n.p$$

4.5.3 Démonstration dans le cas général

Soit G un groupe fini ; soit H un sous-groupe de G ; on définit sur G une relation d'équivalence ainsi :

$$x \sim y \text{ si } x.y^{-1} \in H$$

Remarque

C'est une généralisation de la construction de $\mathbb{Z}/n\mathbb{Z}$: voir **3.1**

En effet, pour construire $\mathbb{Z}/n\mathbb{Z}$, on défnit

$$x \sim y \text{ si } x - y \in n\mathbb{Z}$$

Cherchons les classes d'équivalence

$$\forall x \in G, x \in \overline{a} \Longleftrightarrow \exists h \in H, x.a^{-1} = h \Longleftrightarrow \exists h \in H, x = h.a$$

Donc

$$\overline{a} = \{h.a / h \in H\} = Ha$$

Leur cardinal

$h \to h.a$ est une bijection entre H et Ha ; les classes d'équivalence ont donc pour cardinal celui de H.

Le nombre d'éléments de G est donc le nombre de classes n_c multiplié par le cardinal commun aux classes, celui de H :

$$|G| = |H| \, .n_c$$

Conclusion

On a montré le théorème de Lagrange (HP) :

Le cardinal de tout sous-groupe H de G divise le cardinal de G.
En particulier, l'ordre de tout élément de G divise le cardinal de G.

4.5.4 Les groupes de cardinal premier

Exercice

Soit G un groupe de cardinal p premier ; montrer que G est cyclique.

Démonstration

Soit $a \in G - \{e\}$; l'ordre q de a divise p, p est premier, donc $q = p$ ou $q = 1$.

Mais seul e_G est d'ordre 1 ; donc a est d'ordre p.

4.5.5 Les groupes de cardinal 4

Exercice

Soit G un groupe de cardinal 4 non cyclique.

Montrer qu'il contient 3 éléments a, b, c d'ordre 2.
Montrer que G est abélien.
Montrer que $ab = c$.
Montrer que G est isomorphe à $\mathbb{U}_2 \times \mathbb{U}_2$.

4.6 Ordre dans S_n

4.6.1 Cycle

Soit $\sigma = (a_1 \ a_2 \ ... \ a_p)$ un cycle ; quel est son ordre ?

4.6.2 Cas général

L'ordre d'une permutation σ est ?

Réponse

Le PPCM des ordres des cycles.

4.7 Les groupes de cardinal pair

Exercice

Si G est un groupe de cardinal pair, G contient un élément d'ordre 2.

Démonstration

Le nombre d'éléments égaux à leur inverse est pair, et non nul : il y a au moins e_G ; donc il y en a au moins un autre, qui est donc d'ordre 2.

4.8 Les sous-groupes de cardinal $n/2$

Exercice

Soit G un groupe fini de cardinal n et H un sous-groupe de cardinal p tel que $n = 2p$.

Que dire de aH ? de Ha ?

Réponse

Si $a \in H$, $aH = H = Ha$; sinon $aH = Ha = G \setminus H$.

Conséquence :

$$\forall a \in G,\ aH = Ha$$

$$\forall a \in G,\ aHa^{-1} = H$$

H est donc invariant par tout automorphisme intérieur (sous-groupe appelé invariant, ou distingué).

5 Exercices sur $\mathbb{U}_n$ et les groupes cycliques

5.1 Les sous-groupes finis de $\mathbb{C}^*$

Exercice

Les seuls sous-groupes finis de $\mathbb{C}^*$ sont les $\mathbb{U}_n$, $n \geq 1$.

Démonstration

Soit G un sous-groupe fini de $\mathbb{C}^*$; soit n son cardinal.

Il suffit de montrer que $G \subset \mathbb{U}_n$.

Soit $z \in G$; $z^n = 1$ car l'ordre de z divise le cardinal de G ; donc

$$z \in \mathbb{U}_n$$

Remarque

Des sous-groupes infinis de $\mathbb{C}^*$:

$\mathbb{R}^*$, $\mathbb{Q}^*$, $]0, +\infty[$, $\{2^n / n \in \mathbb{Z}\}$, $\mathbb{U}$, la réunion des $\mathbb{U}_n$: $\bigcup_{n\geq 1} \mathbb{U}_n$...

5.2 Inclusion

A quelle condition $\mathbb{U}_p \subset \mathbb{U}_q$?

Réponse

$\mathbb{U}_p \subset \mathbb{U}_q$ si et seulement si $\omega_p = \exp\left(\frac{2i\pi}{p}\right) \in \mathbb{U}_q$.

Or $\omega_p^q = \exp\left(\frac{2i\pi q}{p}\right) = 1$ si et seulement si p divise q.

5.3 Intersection

$\mathbb{U}_p \cap \mathbb{U}_q$?

Réponse

On remarque que $z \in \mathbb{U}_p$ si et seulement si l'ordre de z divise p.

Donc $z \in \mathbb{U}_p \cap \mathbb{U}_q$ si et seulement si l'ordre de z divise $d = p \wedge q$.

Conclusion :

$$\mathbb{U}_p \cap \mathbb{U}_q = \mathbb{U}_d$$

5.4 Produit

On suppose que $p \wedge q = 1$; montrer que $\mathbb{U}_p \times \mathbb{U}_q$ et $\mathbb{U}_{pq}$ sont isomorphes.

Réponse

Soit

$$\begin{array}{c} f : \mathbb{U}_p \times \mathbb{U}_q \to \mathbb{U}_{pq} \\ (x, y) \to xy \end{array}$$

On cherche son noyau :

si $(x, y) \in \ker f$, $x.y = 1$, donc

$$x = y^{-1} \in \mathbb{U}_p \cap \mathbb{U}_q = \{1\}$$

Finalement :

$$(x, y) = (1, 1)$$

Remarque : il en découle que le produit de deux groupes cycliques dont les cardinaux sont premiers entre eux est cyclique.

5.5 Les endomorphismes de groupe de $\mathbb{U}_n$

Il y en a n ; ce sont les $f_q : x \to x^q$ pour $1 \leq q \leq n$.

Démonstration

On vérifie facilement que les f_q sont des morphismes de groupes ; montrons que ce sont les seuls :

Soit f un endomorphisme de groupe de $\mathbb{U}_n$; soit $\omega = \exp\left(\frac{2i\pi}{n}\right)$; soit $a = f(\omega)$; a est dans $\mathbb{U}_n$, donc a s'écrit

$$a = \exp\left(\frac{2i\pi q}{n}\right) = \omega^q$$

Il reste à montrer que ?

Il reste à montrer que $f = f_q$. Or, $f(x) = f_q(x)$ est vérifié pour $x = \omega$. Pour un x quelconque ?

On écrit $x = \omega^k$; d'où

$$f(x) = f\left(\omega^k\right) = f(\omega)^k = a^k = x^q$$

Que reste-t-il à montrer ?

Que les morphismes trouvés sont distincts.

Remarque

Lesquels sont des automorphismes ?

Les f_q avec $n \wedge q = 1$.

5.6 Sous-groupes d'un groupe cyclique

Soit G un groupe cyclique, et H un sous-groupe de G ; alors H est cyclique.

Démonstration

Supposons $G = \mathbb{U}_n$; H est alors un sous-groupe fini de $\mathbb{C}^*$; d'après un exercice, H est l'un des $\mathbb{U}_k$.

Donc H est cyclique.

5.7 L'ordre de $\omega = \exp\left(\frac{2ik\pi}{n}\right)$

On cherche l'ordre de $\omega = \exp\left(\frac{2ik\pi}{n}\right)$, avec $n \geq 1$ et k entier quelconque.

On sait déjà qu'il divise n car $\omega^n = 1$.

Cas où $k \wedge n = 1$.

Soit q l'ordre de ω ; $\omega^q = 1$; donc n divise $k.q$.

Avec le théorème de Gauss : n divise q.

Conclusion :

$$n = q$$

Cas général

Soit $d = n \wedge k$; on sait que

$$n = d.n'$$
$$k = d.k'$$

avec $n' \wedge k' = 1$.

On est donc ramené au cas précédent : l'ordre de ω est

$$n' = \frac{n}{n \wedge k}$$

5.8 L'ordre de ab

Soit a et b deux éléments d'un groupe G.

Si a est d'ordre p, b d'ordre q, $p \wedge q = 1$, et $a.b = b.a$, alors $a.b$ est d'ordre pq.

Démonstration

Soit $n \geq 1$; supposons

$$(ab)^n = e$$

Alors

$$a^n = b^{-n}$$

Que dire de l'ordre de cet élément $c = a^n$?

$$c \in \langle a \rangle \cap \langle b \rangle$$

L'ordre de c divise p et q, donc $c = e$:

$$a^n = b^{-n} = e$$

On en déduit que n est un multiple de p et de q, donc de pq.

6 Groupes d'isométries

Soit A une partie finie de $E = \mathbb{R}^2$; soit G l'ensemble des isométries de E laissant A invariant ; G est un groupe : sous-groupe de l'ensemble des isométries de E.

6.1 A est un rectangle

G est de cardinal 4, isomorphe à $\mathbb{U}_2^2$.

6.2 A est un triangle équilatéral

G est de cardinal 6, isomorphe à S_3.

6.3 A est un carré

G est de cardinal 8 ; il contient un sous-groupe isomorphe à $\mathbb{U}_4$.

On note $G = D_4$: groupe diédral.

Groupes de cardinal 8

Il y a donc au moins 4 groupes de cardinal 8 non isomorphes.

En fait, il y en a un 5e : le groupe des quaternions H.

7 Exercices sur S_n

7.1 $\sigma = (1\ 2\ 3 \ldots n)$

Soit $\sigma = (1\ 2\ 3 \ldots n) \in S_n$; σ^2 est-il un cycle ?

Réponse

Si $n = 2p + 1$

$$(1\ 2\ \ldots\ 2p+1)^2 = (1\ 3\ \ldots\ 2p+1\ 2\ \ldots\ 2p)$$

Si $n = 2p$:

$$(1\ 2 \ldots 2p)^2 = (1\ 3\ \ldots\ 2p-1) \circ (2\ 4\ \ldots\ 2p)$$

7.2 A_n

On note $A_n = \ker\varepsilon$ (le groupe alterné) ; quel est son cardinal ?

Réponse

Si $n \geq 2$, $|A_n| = \frac{n!}{2}$. En effet, soit

$$f_0 \in S_n - A_n$$

L'application

$$f \to f \circ f_0$$

induit une bijection de A_n sur $S_n - A_n$.

C'est un cas particulier de l'exercice **2.8** et une illustration de **4.8**

7.3 Conjugué d'un cycle

Soit $c = (e_1\, e_2 \ldots e_p)$ un cycle, et σ un élément de S_n.

Que dire de

$$\sigma \circ c \circ \sigma^{-1}$$

Réponse

$$\sigma \circ c \circ \sigma^{-1} = (\sigma(e_1)\ \sigma(e_2)\ \ldots \sigma(e_p))$$

7.4 Centre de S_n

Si $n \geq 3$:

$$Z(S_n) = \{\mathrm{Id}\}$$

Démonstration

Soit σ élément du centre de S_n ; soit $t = (i\, j)$ une transposition.

$$\sigma \circ t \circ \sigma^{-1} = (\sigma(i)\ \sigma(j))$$

Et après ?

$$(i\, j) = (\sigma(i)\ \sigma(j))$$

Donc

$$\sigma(i) \in \{i, j\}$$

Soit k différent de i et de j ; pour les mêmes raisons

$$\sigma(i) \in \{i, k\}$$

Donc $\sigma(i) = i$, et i est quelconque. Conclusion :

$$\sigma = \mathrm{Id}$$

7.5 Morphismes de S_n dans $\mathbb{C}^*$

Soit φ un morphisme de groupes de S_n dans $\mathbb{C}^*$.

1- Soit t une transposition. Montrer que $\varphi(t) = \pm 1$.

Soit t et t' deux transpositions.

2- Montrer qu'elles sont conjuguées dans S_n.

3- Montrer que $\varphi(t) = \varphi(t')$.

4- Conclure.

7.6 Les groupes de cardinal 6

1e méthode

Soit G un groupe non commutatif de cardinal 6. Montrer que

- G contient un élément a d'ordre 3 ; on note $H = \{e, a, a^2\}$.
- G contient un élément b d'ordre 2.
- $b^{-1}Hb = H$.
- $b^{-1}ab = bab = a^2$.
- Déterminer la table de G et conclure que G est isomorphe à S_3.

2e méthode

Soit G un groupe non commutatif de cardinal 6.

- Montrer que G contient un sous-groupe H de cardinal 3. On note

$$A = G \setminus H$$

- Pour $g \in G$, on pose $\varphi_g : x \to g.x.g^{-1}$; montrer que φ_g induit une permutation de A.

- Montrer que $g \to \varphi_g$ induit un isomorphisme de G sur S_A, groupe des permutations de A.

8 Complément : le théorème de Cauchy

8.1 Enoncé

Soit G un groupe fini de cardinal n ; soit p un diviseur premier de n.

Alors G possède au moins un élément d'ordre p.

8.2 Le cas $p = 2$

Déjà vu.

8.3 Le cas général

1e étape

Soit

$$E = \{(x_1, ..., x_p) \in G^p / \, x_1.x_2...x_p = e\}$$

Quel est le cardinal de E ?

Réponse

$$|E| = n^{p-1}$$

2e étape

Soit

$$\begin{array}{rccc} \varphi : & E & \to & E \\ & (x_1, ..., x_p) & \to & (x_2, x_3, ..., x_p, x_1) \end{array}$$

Que dire de φ ?

Réponse

On vérifie d'abord que $\varphi(E) \subset E$; ensuite, $\varphi^p = \mathrm{Id}$, ce qui entraîne que φ est une bijection.

3e étape

Que dire des éventuels éléments de G d'ordre p ?

Réponse

Les points fixes de φ sont les $(a, a, ..., a)$ avec a d'ordre 1 ou p.

4e étape

Conclure.

Réponse

- On sait que $|E|$ est un multiple de p.
- $\varphi^p = \mathrm{Id}$, donc φ est d'ordre 1 ou p. Donc les orbites (les cycles disjoints) sont de cardinal 1 ou p.
- Il y a au moins une orbite de cardinal 1 ; donc il y en a au moins p.

Donc il y a au moins $p-1$ points fixes correspondant à des éléments d'ordre p.

9 Complément : l'exposant d'un groupe abélien fini

Soit G un groupe abélien fini, de cardinal n. On appelle exposant de G le plus petit entier $q \geq 1$ vérifiant

$$\forall x \in G,\ x^q = e$$

9.1 Exemples

q existe :

c'est le plus petit commun multiple des ordres des éléments de G. Remarque : q divise n.

Que vaut q si G est cyclique ?

Que vaut q si $G = \mathbb{U}_m \times \mathbb{U}_n$?

9.2 Il existe un élément d'ordre q

Démonstration

On décompose q en facteurs premiers :

$$q = p_1^{\alpha_1} ... p_r^{\alpha_r}$$

9.2.1 1e étape

Pour chaque j, il existe un élément x_j dont l'ordre est un multiple de $p_j^{\alpha_j}$.

9.2.2 2e étape

Pour chaque j, il existe un élément y_j dont l'ordre est $p_j^{\alpha_j}$.

9.2.3 3e étape

Le produit y des y_j est d'ordre q.

9.3 Application aux corps finis

Soit K un corps, $G \subset (K^*, \times)$ un sous-groupe fini. alors G est alors cyclique.

Remarque

Déjà vu dans le cas où $K = \mathbb{C}$.

Démonstration

Soit q l'exposant de G, et

$$P = X^q - 1$$

On sait que P a au plus q racines dans K, donc dans G.

Et il existe dans G un élément a d'ordre q qui engendre un sous-groupe H cyclique de cardinal q.

Donc :

$$\langle a \rangle = H = G$$