

Notion de groupes

Définitions

- Un groupe est un ensemble G muni d'une loi de composition interne \star vérifiant
 - 1) \star associative : $a \star (b \star c) = (a \star b) \star c$ pour tout a, b, c
 - 2) \star possède un élément neutre e : $e \star a = a \star e = a$ pour tout a
 - 3) Tout élément a possède un symétrique s par \star : $a \star s = s \star a = e$
- Si de plus \star est commutative, le groupe est dit **abélien** : $a \star b = b \star a$ pour tout a, b
- un groupe peut être fini ou infini. S'il est fini son **ordre** est son nombre d'éléments.
- Un groupe peut être **multiplicatif** ($x \star y$ noté xy et symétrique de x ou inverse noté x^{-1}) ou **additif** ($x \star y$ noté $x+y$ et symétrique de x ou opposé de x noté $-x$)
- ensemble réduit à un seul élément e tel que $e \star e = e$ appelé groupe **trivial**
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ dotés de $+$ avec $e = 0$ sont des groupes additifs
- \mathbb{Q}^\star doté de \times avec $e = 1$ est un groupe multiplicatif
- L'ensemble **S(E)** des bijections de E sur E doté de \circ est un groupe multiplicatif dit **symétrique**
- Un ensemble produit de groupes multiplicatifs $G_1 \times G_2 \times \dots \times G_n$ doté de la loi $(x_1, \dots, x_n)(y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n)$ a une structure de groupe multiplicatif. $e = (e_1, \dots, e_n)$, $x^{-1} = (x_1^{-1}, \dots, x_n^{-1})$
- Les **groupes produits** $\mathbb{Z}^n, \mathbb{C}^n, \mathbb{R}^n$ sont des groupes additifs $(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$
- soit G un groupe multiplicatif d'élément neutre e
montrez que si pour tout x on a $x^2 = e$, alors G est abélien
Si G fini d'ordre pair montrez $\exists x \in G$ différent de $e \mid x^2 = e$
- Soit X fini de cardinal n . Quel est l'ordre de $S(X)$? Montrez que X n'est pas commutatif si $n > 2$.

Sous – groupes d'un groupe

- H sous ensemble du groupe G (d'élément neutre e) est un sous groupe de G si
 - 1) $e \in H$
 - 2) tout $x \in H, y \in H$ on a $x \star y \in H$
 - 3) tout $x \in H$ on a symétrique de $x \in H$
- Un sous groupe de G muni de la loi de composition induite par G est un groupe.
- les parties G et $\{e\}$ sont des sous groupes. $\{e\}$ sous groupe trivial
- $\mathbb{R}^{+\star}$ et $\{-1; +1\}$ sont des sous groupes de \mathbb{R}^\star
- L'ensemble des nombres complexes de module 1 est un sous groupe de \mathbb{C}^\star
- **Tous les sous groupes de $(\mathbb{Z}, +)$ sont les ensembles $n\mathbb{Z} = \{nk \mid n \text{ donné } \in \mathbb{Z}, \text{ pour tout } k \in \mathbb{Z}\}$**
- Soit H un sous groupe de \mathbb{Z} , il existe un entier naturel n tel que $H = n\mathbb{Z}$.
- x^k est défini par **1)** $x \dots x$ (k facteurs) si $k > 0$ **2)** e si $k = 0$ **3)** $(x^{-1})^{-k}$ si k est négatif
On a donc ■ $x^a \cdot x^b = x^{a+b}$ ■ $(x^a)^{-1} = x^{-a}$ ■ $(x^a)^b = x^{ab}$
- Il en résulte que $\{x^k \mid k \in \mathbb{Z}\}$ est un sous groupe abélien de G .
- En notation additive la même construction ($nx = x + \dots + x$ avec n termes) donne nG (c.f $n\mathbb{Z}$)
- L'intersection d'une famille de sous groupes de G est un sous groupe de G .
- Montrez que H sous groupe de $G \Leftrightarrow H$ non vide et tous $x, y \in H$ on a $xy^{-1} \in H$
- Montrez que si H et H' sous groupes de G alors $H \cup H'$ sous groupe $\Leftrightarrow H \subset H'$ ou $H' \subset H$
- Si H et K sous groupes de G , $HK = \{ab \mid a \in H \text{ et } b \in K\}$. HK est un sous ensemble de G .
Montrer que $HK = KH \Leftrightarrow HK$ sous groupe de G
- Soit $a, b \in \mathbb{Z}^\star$ montrer que $a\mathbb{Z} \cap b\mathbb{Z} = (\text{PPCM}(a, b))\mathbb{Z}$

Classes modulo un sous groupe

- Soit G **groupe multiplicatif** d'élément neutre e et H un sous groupe de G
 R définie par $xRy \Leftrightarrow x^{-1}y \in H$ est une relation d'équivalence sur G . (Réflexive, symétrique, transitive)
- Soit x un élément de G , sa classe d'équivalence est $xH = \{xh \mid h \in H\}$.
En effet pour tout xh on a $x^{-1}xh = h \in H$ donc tout xh est en relation avec x (équivalent à x).
- xH est **la classe à gauche de x modulo H** .
L'ensemble des classes à gauche des éléments de G modulo H se note G/H . (**ensemble quotient à gauche de G modulo H**). $G/H = \{xH \mid x \in G\}$
- **Théorème de LAGRANGE** : si G est un groupe fini, H et G/H le sont aussi.
On a **$\text{card}(G) = \text{card}(H) \cdot \text{card}(G/H)$** . L'ordre de H divise celui de G . ($\text{card}(G)$ peut être noté $|G|$)
- **Corollaire** si G est fini d'ordre premier alors ses seuls sous groupes sont G et $\{e\}$.
- Si G **abélien** classe à gauche = classe à droite $\rightarrow R$ s'appelle relation d'équivalence modulo H .
 xH s'appelle **classe d'équivalence modulo H** et G/H **ensemble quotient de G modulo H** .
- Dans le cas d'un **groupe additif** : xRy s'écrit $xRy \Leftrightarrow x - y \in H$, la classe de x modulo H est $x+H$, avec $x+H = \{x+h \mid h \in H\}$ et $G/H = \{x+H \mid x \in G\}$ et on remarque que $0+H = H$.
- **L'ensemble $\mathbb{Z} / n\mathbb{Z}$**

Si $G = \mathbb{Z}$, $H = n\mathbb{Z}$ avec $n \in \mathbb{N}^*$ et $xRy \Leftrightarrow x - y \in n\mathbb{Z}$ autrement dit $x - y$ est divisible par n .

On dit que **x congru à y modulo n** . on l'écrit $x \equiv y \pmod{n}$. Classe de $x = \bar{x} = \{x+nk \mid k \in \mathbb{Z}\}$

Si r est le reste de la division de x par n on a $x \equiv r \pmod{n}$

$\mathbb{Z} / n\mathbb{Z} = \{\bar{x} \mid x \in \mathbb{Z}\} = \{\text{ensemble des classes des restes possibles}\} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

La surjection canonique est la surjection qui à $x \in \mathbb{Z} \rightarrow \bar{x} \in \mathbb{Z} / n\mathbb{Z}$ (bijection si $n = 0$)

Groupes quotient d'un groupe abélien

- G groupe abélien additif d'élément neutre 0 . H sous groupe de G . $G/H = \{x+H \mid x \in G\}$
Soit $u, v \in G/H$. Soit, dans G , $x \in u$ et $y \in v$. On définit $u \oplus v = x+y+H$.
On démontre que $u \oplus v$ est identique si on choisit un autre couple (x', y') tel que $x' \in u$ et $y' \in v$.
 $u \oplus v$ est donc la classe de $x+y \pmod{H}$. Et \oplus est une loi de composition interne sur G/H .
- L'ensemble G/H muni de \oplus est un groupe abélien: On l'appelle **groupe quotient de G par H** .
- D'après Lagrange si G est fini, G/H est fini d'ordre $\text{card}(G) / \text{card}(H)$.
- **Le groupe additif $(\mathbb{Z} / n\mathbb{Z}, \oplus)$**

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

Par abus on peut remplacer la notation \oplus par $+$. $(\mathbb{Z} / n\mathbb{Z}, +)$ vérifie:

$$\begin{array}{llll} \blacksquare \bar{a} + \bar{b} = \overline{a+b} & \blacksquare \text{élément neutre } \bar{0} & \blacksquare -\bar{a} = \overline{-a} & \blacksquare k\bar{a} = \overline{ka} \quad (\text{tout } k \in \mathbb{Z}) \end{array}$$

- ▣ Montrer que $\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$ est un sous groupe de $\mathbb{Z} / 12\mathbb{Z}, +$
- ▣ Expliciter un sous groupe d'ordre 6 de $\mathbb{Z} / 12\mathbb{Z}, +$
- ▣ Déterminer tous les sous groupes de $\mathbb{Z} / 6\mathbb{Z}, +$

Sous groupes engendrés par un élément. Ordre d'un élément.

- Soit $x \in G$. On appelle **sous groupe engendré par x** (noté $\langle x \rangle$) l'intersection de tous les sous groupes qui contiennent x . Autrement dit le plus petit sous groupe contenant x .
- On a l'égalité $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$
- Exemple 1 : dans $\mathbb{Z}, +$ le sous groupe engendré par n est $n\mathbb{Z}$

Exemple 2 : dans $\mathbb{Z}/n\mathbb{Z}$ si $n \geq 1$ le sous groupe engendré par $\bar{1}$ est $\mathbb{Z}/n\mathbb{Z}$ tout entier

► Désormais on s'intéresse au cas de **G fini**

- Tout $x \in G$, par définition **ordre de $x =$ ordre de $\langle x \rangle =$ plus petit entier k tel que $x^k = e$**
- Soit $x \in G$ d'ordre m . On a
 - 1) $m \geq 1$ et m divise l'ordre de G
 - 2) $x^m = e$ et m est le plus petit entier tel que $x^m = e$
 - 3) Pour $1 \leq k \leq m$, tous les x^k sont distincts et $\langle x \rangle = \{x^1; x^2; \dots; x^{m-1}; x^m = e\}$

Exemple dans $G = \mathbb{Z}/20\mathbb{Z}$ $\{3n\} = G$ (ordre de 3 = 20) $\{2n\} = \{\text{classes paires}\}$ (ordre de 2 = 10)
 $\{5n\} = \text{classes } \{5; 10; 15; 0\}$ (ordre de 5 = 4 et $4 \times 5 = 0$)

- Si G fini d'ordre n alors pour tout x de G on a $x^n = e$.

- Soit $x \in G$ d'ordre m

1) Si $k \in \mathbb{N}$ et $x^k = e$, alors m divise k

2) pour tout entier k on a : ordre de $x^k = \frac{m}{\text{PGCD}(m,k)}$

- Soit $x \in G$ et $m \geq 1$ on a l'équivalence

ordre de $x = m \iff x^m = e$ et pour tout diviseur premier p de m on a $x^{\frac{m}{p}} \neq e$

- Corollaire: si a et n entiers tels que $0 \leq a \leq n-1$, dans $\mathbb{Z}/n\mathbb{Z}, +$ l'ordre de \bar{a} est $\frac{n}{\text{PGCD}(n,a)}$.

■ démontrer que tout $x \in G$, x et x^{-1} ont le même ordre

■ Si, $x, y, g \in G$ et $y = gxg^{-1}$ alors x et y sont dits conjugués. Démontrez qu'ils sont du même ordre.

Il en résulte que pour tout a, b de G les ordres de ab et ba sont égaux ($a^{-1}(ab)a = ba$)

Attention! en général (ordre de ab) \neq (ordre de a)(ordre de b)

■ Quel est l'ordre de $\bar{2}$ dans $\mathbb{Z}/10\mathbb{Z}, +$?

■ Soit G_1, G_2 groupes finis, soit $(x, y) \in G_1 \times G_2$,

montrer ordre de $(x, y) = \text{PPCM}(\text{ordre de } x, \text{ordre de } y)$

■ Soit G groupe abélien fini. P le produit de tous ses éléments. Montrez $P^2 = e$

Calculez S (somme de tous les éléments) dans le cas $\mathbb{Z}/n\mathbb{Z}$ avec $n \geq 1$.

Groupes cycliques. Fonction indicatrice d'Euler.

- G fini d'ordre n est **cyclique** si $\exists x \mid \langle x \rangle = G$. Dans ce cas, G est aussi abélien.
- G cyclique $\Leftrightarrow \exists x \in G$ d'ordre n et pour x d'ordre n on a $G = \{x^1; x^2; \dots; x^{n-1}; x^n = e\}$
- Exemples : $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n

$\{\exp(\frac{2ki\pi}{n}) \mid 0 \leq k \leq n-1\}$ cyclique d'ordre n dans \mathbb{C}^* et de générateur $\exp(\frac{2i\pi}{n})$

$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, +)$ cyclique d'ordre 6 et de générateur $(\bar{1}, \bar{1})$

Tout groupe fini d'ordre p premier est cyclique

- Soit G cyclique d'ordre n
 - 1) tout sous groupe de G est cyclique
 - 2) pour tout diviseur d de n les ensembles $H_d = \{x \in G \mid x^d = e\}$ sont sous groupes d'ordre d.
 - 3) l'application $d \rightarrow H_d$ est une bijection sur l'ensemble des sous groupes de G

- pour toute entier m on définit $\varphi(m)$ = nombre d'entiers $k \leq m$ et premiers avec m.

C'est la **fonction indicatrice d'Euler**. $\varphi(1) = 1$. Pour tout nombre premier p: $\varphi(p) = p-1$

- Pour tout nombre premier p et $k \in \mathbb{N}^*$ on a $\varphi(p^k) = p^k - p^{k-1} = p^k (1 - \frac{1}{p})$

(il y a p^k entiers non nuls $\leq p^k$ parmi lesquels p^{k-1} multiples de p et donc non premiers avec p)

- Pour tout entier $m \geq 1$, si on appelle d les diviseurs positifs de m, on a $m = \sum_{\{d\}} \varphi(d)$

Exemple $\varphi(21) = \text{card} \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\} = 12$; $\varphi(1) = 1$; $\varphi(3) = 2$; $\varphi(7) = 6$ et $21 = 12 + 6 + 2 + 1$

- Si G cyclique d'ordre n et x un générateur de G, alors l'ensemble des générateurs de G est $\{x^k \mid 1 \leq k \leq n \text{ et } \text{PGCD}(k, n) = 1\}$

- Si G cyclique d'ordre n et d diviseur de n: il y a exactement $\varphi(d)$ éléments d'ordre d dans G.

- Corollaire: L'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$ est $\{\bar{a} \mid 1 \leq a \leq n \text{ et } \text{PGCD}(1, a) = 1\}$

- Soient a et n entiers premiers entre eux on a : $a^{\varphi(n)} \equiv 1 \pmod{n}$

■ Montrer que tout sous groupe fini de (\mathbb{C}^*, X) est cyclique

■ Pour tout $n \geq 1$ montrer que $\varphi(n)$ divise n!

■ Soit $n \geq 1$, $d(n)$ son nombre de diviseurs. Déterminer $d(n)$ en fonction de la décomposition en facteurs premiers de n. Trouver tous les entiers ≤ 30 tels que $\varphi(n) = d(n)$. (on peut démontrer que pour $n > 30$ on a $\varphi(n) > d(n)$).

Homomorphismes de groupes.

- Déf un **morphisme** ou **homomorphisme** de G, \star dans G', \odot est $f: G \rightarrow G' \mid f(x \star y) = f(x) \odot f(y)$.
 $\log: (\mathbb{R}^{+\star}, \times) \rightarrow (\mathbb{R}, +) \mid \log(xy) = \log(x) + \log(y)$ est un homomorphisme de groupes
 f_a avec $a \in G: (\mathbb{Z}, +) \rightarrow (G, \star) \mid n \in \mathbb{Z} \rightarrow f_a(n) = a^n$ est un homomorphisme car $f(n+n') = a^{n+n'} = a^n \cdot a^{n'}$.
 $s: G$ abélien additif $\rightarrow G/H \mid x \rightarrow s(x) = \bar{x}$ **homomorphisme canonique** $s(x+x') = \overline{x+x'}$
- G et G' d'élément neutre e et e' . $f: G \rightarrow G'$ homomorphisme de groupe on a
 1) $f(e) = e'$ 2) pour tout x de G $f(x^{-1}) = [f(x)]^{-1}$
- Si f et g homomorphismes, alors $f \circ g$ homomorphisme. Si f homomorphisme bijectif f^{-1} homomorphisme
- Déf: Un homomorphisme bijectif est un **isomorphisme**. G et G' sont alors dits **isomorphes**.
 2 ensembles isomorphes ont des structures et des propriétés transposables de l'un à l'autre
- Déf: Un isomorphisme de G sur lui-même est appelé **automorphisme**
- Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}, +$. Pour le démontrer il suffit de choisir g un générateur de G et de définir $f: G \rightarrow \mathbb{Z}/n\mathbb{Z}$ par $f(g^k) = \bar{k}$ (pour $k \in \mathbb{Z}$, g^k décrit G).
- Soit f homomorphisme de G dans G' : 1) si H sous groupe de G alors $f(H)$ sous groupe de G' .
 2) si H' sous groupe de G' alors $f^{-1}(H')$ est un sous groupe de G .
- **Le noyau de f** est $f^{-1}(e')$ c'est-à-dire **$\text{Ker}(f) = \{x \in G \mid f(x) = e'\}$** est un sous groupe. $e \in \text{ker}(f)$
 f **injective** $\Leftrightarrow \text{ker}(f) = \{e'\}$.
- Si $G, +$ est abélien alors $G/\text{Ker}(f)$ isomorphe à $f(G)$ via l'application $s: s(\bar{x}) = f(x)$
- **CAUCHY**: G abélien fini d'ordre n , p diviseur premier de $n \rightarrow \exists x \in G$ d'ordre p .
- Si $n =$ produit de facteurs premiers à exposants < 2 . Alors G abélien d'ordre n est cyclique d'ordre n .
- Puissances de x dans un groupe G cyclique d'ordre n

notation x Si $x \in G: x^k = a \Leftrightarrow a^{\frac{n}{d}} = e$ avec $d = \text{PGCD}(k, n)$

notation + $kx = a \Leftrightarrow \frac{n}{d}a = e$ avec $d = \text{PGCD}(k, n)$

exemple dans $\mathbb{Z}/60\mathbb{Z}$ ($n=60$), $k=35$, $a=20$, $x=4$ $\text{PGCD}(35, 60)=5$ on a $35(4) = 20 \Leftrightarrow \frac{60}{5}20 = 240=0$

notation x Si $x_0^k = a$ alors l'ensemble des solutions de $x^k = a = \{x_0 z \mid z \in G \text{ et } z^k = e\}$ (k solutions)

notation + Si $kx_0 = a$ alors ensemble des solutions de $kx = a = \{x_0 + z \mid z \in G \text{ et } kz = 0\}$ (k solutions)

● Plus généralement si f automorphisme et si x_0 est solution de $f(x) = a$, alors toutes les solutions sont de type $x_0 \star y$ avec $y \in \text{ker}(f)$.

Exemple: $G = \mathbb{Z}/25\mathbb{Z}$. Quelles sont dans G les solutions de $5x = \overline{15}$?

Dans ce groupe on a $5x = \overline{0}$ pour $x = \overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}$

et $\overline{3}$ est une solution particulière de $5x = \overline{15}$

donc toutes les solutions sont les classes $\{3+0, 3+5, 3+10, 3+15, 3+20\}$

■ Dans $\mathbb{Z}/1000\mathbb{Z}$ résoudre l'équation $5x = \overline{50}$

En résumé Groupes finis

- Card (G) encore noté $|G|$ est l'ordre du groupe
- il existe un ou plusieurs entiers non nuls, k tel que pour tout $a \in G$ on a $a^k = e$ (1 en notation multiplicative)
- le plus petit k pour lequel on a $a^k = e$ est l'ordre de a
- l'ordre de a divise les autres entiers k pour lesquels on a $a^k = e$
- On a aussi $a^{-1} = a^{(\text{ordre de } a) - 1}$
- Un sous ensemble S de G engendre G si tout élément de G peut s'écrire comme une combinaison d'éléments de S (ou de leurs symétriques).
- Un groupe (fini ou pas) engendré par un seul élément g est dit cyclique (on note $G = \langle g \rangle$)
- un groupe cyclique est nécessairement abélien
- Si g générateur de G cyclique on a ordre de $G =$ ordre de g
- Si H sous groupe de G fini alors l'ordre de H divise l'ordre de G (Lagrange)
- En conséquence si G est fini d'ordre m pour tout a de G on a $a^m = e$