

Groupes

1. Notions de base
2. Quotients de groupe
3. Quelques groupes particuliers
4. Actions de groupe
5. Théorèmes de Sylow

§1. Notions de base

Définition

Un **groupe** est un ensemble non vide G avec opération $*$ interne vérifiant

1. (élément neutre) $\exists e \in G$ avec $x * e = e * x = x \quad \forall x \in G$
2. (associativité) $\forall x, y, z \in G, x * (y * z) = (x * y) * z = x * y * z$
3. (invertibilité) $\forall x \in G, \exists x' \in G$ avec $x * x' = x' * x = e$

Remarques

- ▶ *L'élément neutre et l'inverse de x (pour x donné) sont uniques*
- ▶ *Le groupe est abélien (commutatif) si, $\forall x, y \in G, x * y = y * x$,*
- ▶ *Notations usuelles : multiplicative ou additive (abélien)*

Résultat. Soient $x, y, z \in G, xz = yz \implies x = y$ (simplification) et $(xy)^{-1} = y^{-1}x^{-1}$ (inversion inverse l'ordre)

Définition

Soient $x \in G$ et $n \in \mathbb{Z}$, on pose

$$x^n = \begin{cases} e & \text{si } n = 0 \\ \underbrace{x \cdot x \cdots x \cdot x}_{n \text{ termes}} & \text{si } n > 0 \\ \underbrace{x^{-1} \cdot x^{-1} \cdots x^{-1} \cdot x^{-1}}_{-n \text{ termes}} & \text{si } n < 0 \end{cases}$$

Résultat. Soient $x \in G$ et $n, m \in \mathbb{Z}$, $x^n x^m = x^{n+m}$ et $(x^n)^m = x^{nm}$

Résultat. Soient $x, z \in G$ et $n \in \mathbb{Z}$, $(zxz^{-1})^n = zx^n z^{-1}$

Définition

Soit $x \in G$, le plus petit $n \geq 1$ tel que $x^n = e$ est l'**ordre** de x (ordre fini).

Si n n'existe pas, alors x est d'**ordre infini**.

Définition

Soit $x \in G$, le plus petit $n \geq 1$ tel que $x^n = e$ est l'**ordre** de x (ordre fini).
Si n n'existe pas, alors x est d'**ordre infini**.

Lemme

Soit $x \in G$ d'ordre fini $n \geq 1$. On a

- Pour $t \in \mathbb{Z}$, $x^t = e$ si et seulement si n divise t .
- Pour $\ell \in \mathbb{Z}$, l'ordre de x^ℓ est fini et est égal à

$$\frac{n}{\text{PGCD}(n, \ell)}$$

Soit $y \in G$ d'ordre fini $m \geq 1$ tel que x et y commutent alors l'ordre de xy divise $\text{PPCM}(n, m)$.

Remarque

Si le groupe G est fini alors tous les éléments de G sont d'ordre fini

Définition

Un **sous-groupe** est un sous-ensemble non vide stable par l'opération $*$ et l'inversion (contient forcément e)

Sous-groupes particuliers.

- **Centre** du groupe G : $Z(G) = \{x \in G : \forall g \in G, xg = gx\}$

Note. $G = Z(G)$ ssi G est abélien.

- Pour H sous-groupe de G , le **centralisateur** de H :

$$Z_H(G) = \{x \in G : \forall h \in H, xh = hx\}.$$

Note. $H \subseteq Z_H(G)$ ssi H est abélien.

- Pour H sous-groupe de G , le **normalisateur** de H :

$$N_H(G) = \{x \in G : \forall h \in H, xhx^{-1} \in H\}.$$

Note. $xh = hx \iff xhx^{-1} = h$ donc $Z_H(G) \subseteq N_H(G)$.

Définition

Soit S une partie de G , on note $\langle S \rangle$ le plus petit sous-groupe de G contenant S . On l'appelle le **sous-groupe engendré** par S . Si $\langle S \rangle = G$, on dit que S est **générateur**.

Si $S = \{g\}$, on note plutôt $\langle g \rangle$. Un groupe est **monogène** s'il est engendré par un seul élément.

Résultat. $\langle S \rangle$ est l'intersection des sous-groupes de G contenant S , c'est aussi l'ensemble des produits de la forme

$$s_1^{a_1} s_2^{a_2} \cdots s_t^{a_t} \text{ avec } t \geq 0, s_i \in S, a_i = \pm 1$$

Proposition

Soit $g \in G$. Si g est d'ordre infini alors le groupe $\langle g \rangle$ est de cardinal infini. Si g est d'ordre fini égal à n , alors le cardinal de $\langle g \rangle$ est n , plus exactement

$$\langle g \rangle = \{g^0 = e, g, g^2, \dots, g^{n-1}\}$$

Définition

L'**ordre** d'un groupe G est le cardinal du groupe G . On note $|G|$.

Définition

Soient G_1 et G_2 deux groupes. Une application $f : G_1 \rightarrow G_2$ est un **morphisme** (de groupes) si, $\forall x, y \in G_1$, $f(xy) = f(x)f(y)$. Si, de plus, f est bijective, on dit que f est un **isomorphisme** et on note $G_1 \simeq G_2$. Une isomorphisme entre G et lui-même est un **automorphisme**.

Remarque

*L'ensemble des automorphismes de G est un groupe pour la composition dénoté **Aut(G)**.*

Proposition

Soit $f : G_1 \rightarrow G_2$ un morphisme de groupes. Alors, les ensembles

$$\begin{aligned}\text{Im}(f) &= \{f(x) : x \in G_1\} && \text{image de } f \\ \text{Ker}(f) &= \{x \in G_1 \text{ tel que } f(x) = e_2\} && \text{noyau de } f\end{aligned}$$

sont des sous-groupes de G_2 et G_1 resp. De plus, f est surjective ssi $\text{Im}(f) = G_2$ et injective ssi $\text{Ker}(f) = \{e_1\}$.

Partie génératrice de $GL_n(k)$.

Matrices élémentaires $E_{i,j} = (0 \text{ partout sauf } 1 \text{ en ligne } i, \text{ colonne } j)$.

Matrices de dilatations

$$I_n + \lambda E_{i,i} = \text{diag}(1, \dots, 1 + \lambda, \dots, 1) \quad \text{avec } \lambda \neq -1$$

Matrices de transvections

$$I_n + \lambda E_{i,j} \quad \text{avec } \lambda \neq 0, \ i \neq j$$

Théorème

L'ensemble des matrices de dilatation et des matrices de transvection engendrent le groupe (multiplicatif) $GL_n(k)$.

Partie génératrice de $O_n(k)$.

Matrice orthogonale. $M^t M = I_n \iff M$ inversible et $M^{-1} = {}^t M$.

Une **Reflexion orthogonale** est (la matrice d') une symétrie orthogonale par rapport à un hyperplan.

Soit H hyperplan de k^n (= s.e.v. de dim $n - 1$), tout $v \in k^n$ se décompose $v = h + p$ avec $h \in H$ et $p \perp H$ (d'où $p = 0$ ou $p \notin H$). La réflexion correspondante est la fonction $x \mapsto h - p$.

Théorème

L'ensemble des réflexions orthogonales engendre le groupe (multiplicatif) $O_n(k)$ (qui est un sous-groupe de $GL_n(k)$).

2. Quotients de groupe

Notation. Pour $A \subset G$ et $g \in G$. On pose $gA = \{ga : a \in A\}$ (idem pour Ag). C'est un sous-ensemble de G .

Définition

Soit H sous-groupe de G . Relation d'équivalence sur G :

$$x \sim_H y \quad \text{ssi} \quad xH = yH \quad (\Longleftrightarrow y^{-1}x \in H).$$

On note G/H l'**ensemble quotient** ou encore **ensemble des classes à gauche**, c'est-à-dire $G/H = \{gH : g \in G\}$.

Remarques

- ▶ On définit de même $H \backslash G$ l'ensemble des classes à droites.
- ▶ Toutes les classes ont le même cardinal qui est l'ordre de H .
- ▶ Une autre relation d'équivalence importante est $x \sim y$ si $\exists g \in G$ avec $x = yg^{-1}$ qui donne les **classes de conjugaison**

Théorème (Lagrange)

On a $\text{card}(G/H) = \text{card}(H \backslash G)$ et $|G| = \text{card}(G/H) |H|$.

En particulier, si $|G|$ est fini, l'ordre de tout sous-groupe de G et de tout élément de G divise $|G|$.

*On appelle $\text{card}(G/H)$ l'**indice** de H dans G .*

Remarque. La réciproque est fautive en général : si d divise l'ordre de G , il n'existe pas forcément d'élément ou de sous-groupe de G d'ordre d . (Cas particulier : d premier, G cyclique).

Application au petit théorème de Fermat.

L'ensemble $(\mathbb{Z}/p\mathbb{Z})^\times$ des classes inversibles modulo p avec p premier est un groupe multiplicatif d'ordre $p - 1$ et donc pour tout $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$, on obtient $\bar{a}^{p-1} = \bar{1}$, c'est-à-dire pour tout entier a non divisible par p

$$a^{p-1} \equiv 1 \pmod{p}.$$

Définition

H de G est **distingué** si, $N_H(G) = G$, ie $\forall g \in G, \forall h \in H, ghg^{-1} \in H$
($\iff \forall g \in G, gHg^{-1} \subseteq H \iff \forall g \in G, gHg^{-1} = H$).

On note $H \triangleleft G$

Résultat. Le noyau d'un morphisme est un sous-groupe distingué

Résultat. L'intersection de sous-groupes distingués est un sous-groupe distingué

Théorème

Soit $H \triangleleft G$ alors G/H avec l'opération $aH \cdot bH = abH$ est un groupe et l'application de $G \rightarrow G/H$ définie par $g \mapsto gH$ est un morphisme surjectif de noyau H .

De plus, si $f : G \rightarrow G'$ est un morphisme alors on a

$$G/\text{Ker}(f) \simeq \text{Im}(f) \quad (\text{Théorème de factorisation})$$

Quelques applications du théorème de factorisation

1. Reconnaître les groupes suivants :

$$S_n/A_n, \quad O_n(\mathbb{R})/SO_n(\mathbb{R}), \quad GL_n(\mathbb{R})/SL_n(\mathbb{R}), \quad \mathbb{R}^\times/\mathbb{R}_+^\times.$$

2. Démontrer les isomorphismes suivants :

$$\mathbb{R}/\mathbb{Z} \simeq S_1, \quad \mathbb{R}^\times/\{\pm 1\} \simeq \mathbb{R}_+^\times, \quad \mathbb{C}^\times/S_1 \simeq \mathbb{R}_+^\times$$

avec $S_1 = \{z \in \mathbb{C}^\times : |z| = 1\}$, le cercle trigonométrique.

Sous-groupe caractéristique

Un sous-groupe H est caractéristique dans G s'il est stable par tout automorphisme de G . On note alors $H \sqsubset G$.

1. Montrer qu'un sous-groupe caractéristique dans G est distingué.
2. Démontrer que $H \sqsubset K \sqsubset G \implies H \sqsubset G$.
3. Démontrer que $H \sqsubset K \triangleleft G \implies H \triangleleft G$.
4. Démontrer que le centre d'un groupe est toujours un sous-groupe caractéristique.
5. Soit ϕ l'application qui à $x \in G$ associe l'automorphisme intérieur i_x défini par : $\forall g \in G, i_x(g) = xgx^{-1}$. Montrer que ϕ est un morphisme de groupes. Déterminer son noyau. En déduire l'isomorphisme suivant :

$$G/Z(G) \simeq \text{Int}(G).$$

Définition

Soient H, K sous-groupes de G avec $H \triangleleft G$, G est **produit semi-direct** (interne) de H par K si une des conditions équivalentes est vérifiée

- ▶ $H \cap K = \{e\}$ et $G = HK$
- ▶ Tout élément de $g \in G$ s'écrit de manière unique $g = hk$ avec $h \in H$ et $k \in K$
- ▶ $K \simeq G/H$ via la surjection canonique $k \mapsto kH$

On note $G = H \rtimes K$.

Résultat. On a aussi $G = KH$ et donc $G = K \rtimes H$.

Si on a aussi $K \triangleleft G$, on dit que c'est un **produit direct**.

Dans ce cas, pour tout $k \in K$ et $h \in H$, on a $kh = hk$ et l'application $H \times K \rightarrow G$ définit par

$$(h, k) \mapsto hk$$

est un isomorphisme.

3. Quelques groupes particuliers

Lemme

Soit G un groupe monogène. Si G est infini alors $G \simeq \mathbb{Z}$, sinon G est *cyclique* et $G \simeq \mathbb{Z}/n\mathbb{Z}$ avec n l'ordre de G .

Proposition

Soit $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$. L'ordre de $\bar{m}$ est $n/\text{PGCD}(m, n)$ donc $\bar{m}$ est générateur ssi n et m sont premiers entre eux ssi m est inversible modulo n

Définition

L'ensemble des *inversibles* modulo n forme un groupe multiplicatif

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{m} \text{ tel que } \text{PGCD}(m, n) = 1\}$$

d'ordre $\varphi(n)$ (*fonction indicatrice d'Euler*).

Théorème (Théorème des restes chinois)

Soient n et m deux entiers ≥ 1 et premiers entre eux, on a les isomorphismes naturels

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{et} \quad (\mathbb{Z}/nm\mathbb{Z})^* \simeq (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$$

Nombres d'éléments d'ordre donné dans un groupe cyclique

Soit G un groupe cyclique d'ordre n .

1. Soit $d \geq 1$ un entier. Déterminer le nombre d'éléments d'ordre d dans G .
2. En déduire la formule $\sum_{d|n} \varphi(d) = n$.

Le but de cet exercice est de déterminer la structure du groupe $\text{Aut}((\mathbb{Z}/22\mathbb{Z})^*)$ des automorphismes de $(\mathbb{Z}/22\mathbb{Z})^*$.

1. Déterminer l'ordre de $(\mathbb{Z}/22\mathbb{Z})^*$.
2. Montrer que $\bar{7}$ est un générateur de $(\mathbb{Z}/22\mathbb{Z})^*$. En déduire que $(\mathbb{Z}/22\mathbb{Z})^*$ est cyclique.
3. En déduire tous les sous-groupes de $(\mathbb{Z}/22\mathbb{Z})^*$.
4. Déterminer tous les générateurs de $(\mathbb{Z}/22\mathbb{Z})^*$.
5. Déterminer tous les automorphismes de $(\mathbb{Z}/22\mathbb{Z})^*$.
6. Écrire la table de multiplication de $\text{Aut}((\mathbb{Z}/22\mathbb{Z})^*)$ et en déduire que $\text{Aut}((\mathbb{Z}/22\mathbb{Z})^*)$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Définition

Soit $n \geq 1$, on appelle **groupe symétrique** sur n lettres, l'ensemble $S_n = \text{Bij}(\{1, \dots, n\})$. C'est un groupe pour la composition et son ordre est $n! = 1 \times 2 \times \dots \times n$.

Exemple

Les permutations peuvent s'écrire de deux manières essentiellement

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 5 & 1 & 8 & 7 & 6 \end{pmatrix} \quad (\text{écriture sur deux lignes})$$
$$(1, 4, 5)(2, 3)(6, 8) \quad (\text{produit de cycles disjoints})$$

Remarques

- ▶ La multiplication se fait de droite à gauche $(1, 2)(2, 3) = (1, 2, 3)$
- ▶ On a $(a_1, a_2, \dots, a_s) = (a_2, a_3, \dots, a_s, a_1) = \dots = (a_s, a_1, \dots, a_{s-1})$

Un cycle de longueur ℓ est un **ℓ -cycle** et on appelle un 2-cycle une **transposition**.

Résultat. Les transpositions engendrent S_n .

Lemme

L'ordre d'un ℓ -cycle est ℓ . L'ordre d'une permutation écrit comme produit de cycles disjoints est le PPCM des longueurs des cycles.

Proposition

*Il existe un unique morphisme $\text{sign} : S_n \rightarrow \{\pm 1\}$ non trivial. On l'appelle la **signature**. Soit c un ℓ -cycle, on a $\text{sign}(c) = (-1)^{\ell+1}$.*

*Une permutation π est **paire** si $\text{sign}(\pi) = 1$ et **impaire** si $\text{sign}(\pi) = -1$.*

*Le groupe des permutations paires (= noyau de sign) est le **groupe alterné**, noté A_n . Son ordre est $n!/2$.*

C'est le seul sous-groupe d'ordre $n!/2$ dans S_n .

Remarque

*Un groupe G dont les seuls sous-groupes distingués sont $\{e\}$ et lui-même est un groupe **simple**. Le plus petit groupe simple non abélien est A_5 d'ordre 60 et pour tout $n \geq 5$, le groupe A_n est simple.*

Soit $n \geq 3$. Le **groupe diédral** D_{2n} est le groupe des isométries du plan qui fixe un polygone régulier à n côtés.

C'est un groupe d'ordre $2n$ engendré par la rotation qui envoie un sommet sur le sommet suivant et une des symétries axiales passant par un des sommets.

De manière abstraite, D_{2n} est le groupe engendré par σ et τ avec les relations

$$\sigma^n = e, \quad \tau^2 = e, \quad \tau\sigma\tau = \sigma^{-1}.$$

On a alors

- ▶ Pour tout entier i , $\tau\sigma^i\tau = \sigma^{-i}$.
- ▶ Pour tout entier i , l'élément $\tau\sigma^i$ est d'ordre 2.
- ▶ Les éléments de D_{2n} sont exactement les éléments

$$e, \sigma, \dots, \sigma^{n-1}, \tau, \tau\sigma, \dots, \tau\sigma^{n-1}.$$

4. Actions de groupe

Définition

Une **action** du groupe G sur un ensemble X est la donnée d'un morphisme $\Phi : G \rightarrow \text{Bij}(X)$ (= groupe pour la composition).

En général, on écrit $g \cdot x$ plutôt que $\Phi(g)(x)$ pour $g \in G$ et $x \in X$, d'où

$$\forall x \in X, e \cdot x = x \quad \text{et} \quad \forall g, g' \in G, x \in X, (gg') \cdot x = g \cdot (g' \cdot x).$$

Définition

Pour $x \in X$, on pose

- ▶ $O(x) = \Omega_x = \{g \cdot x : g \in G\}$ est l'**orbite** de x .
- ▶ $S(x) = G_x = \{g \in G \text{ tel que } g \cdot x = x\}$ est le **stabilisateur** de x (sous-groupe de G)

Le **noyau** de l'action est l'intersection des stabilisateurs.

On note X/G l'ensemble des orbites de X .

L'action est **transitive** s'il existe une seule orbite.

L'action est **fidèle** si le noyau est trivial.

Lemme

Soit K le noyau de l'action alors K est distingué et G/K hérite d'une action fidèle sur X

Théorème (Cayley)

Soit G un groupe d'ordre n . Alors G est isomorphe à un sous-groupe de S_n .

Théorème (Formules des classes)

Deux orbites sont ou bien égales, ou bien disjointes, et donc

$$\text{card}(X) = \sum_{\Omega \in X/G} \text{card}(\Omega)$$

Soit $x \in X$, on a

$$\text{card}(\Omega_x) = \frac{|G|}{|G_x|}$$

Soit R un système de représentants des orbites de X , on a

$$\text{card}(X) = \sum_{x \in R} \frac{|G|}{|G_x|}$$

Quelques résultats sur les p -groupes

Un p -groupe, avec p premier, est un groupe fini dont l'ordre est une puissance (non triviale) de p .

1. Soit G un p -groupe. On montre que $Z(G)$ n'est pas réduit à $\{e\}$.

1.1 Soit X un ensemble fini sur lequel G agit. On note X^G l'ensemble des points fixes de X sous cette action. Montrer que

$$\text{card}(X) \equiv \text{card}(X^G) \pmod{p}.$$

1.2 Déterminer une action de G pour laquelle l'ensemble des points fixes est $Z(G)$, puis conclure.

2. Soit G un groupe fini. On suppose que $G/Z(G)$ est un groupe cyclique. Montrer que G est abélien.

En déduire la structure des groupes d'ordre p^2 avec p premier.

Sous-groupes d'indice p avec p plus petit facteur premier de $|G|$

1. Soit H un sous-groupe d'indice 2 dans G . Montrer que $H \triangleleft G$.
2. Soit G un groupe fini. Soit p le plus petit premier divisant $|G|$.

Soit H sous-groupe d'indice p , on montre que $H \triangleleft G$.

On considère l'action de G sur G/H par multiplication à gauche.

2.1 Montrer que cette action est transitive.

2.2 Soit K le noyau de l'action. Montrer que $K \subseteq H$.

2.3 Montrer que G/K est isomorphe à un sous-groupe de S_p .

2.4 En déduire que $H = K$ et le résultat.

Proposition (Lemme de Burnside)

Pour $g \in G$, on pose $X^g = \{x \in X \text{ tel que } g \cdot x = x\}$. On a

$$\text{card}(X/G) = \frac{1}{|G|} \sum_{g \in G} \text{card}(X^g)$$

Problème du collier de perles.

1. Montrer qu'avec 5 perles blanches et 3 perles noires, on ne peut faire que 5 colliers différents de 8 perles.
2. Montrer que le nombre de bracelets de 5 perles qu'on peut faire en utilisant des perles rouges, vertes ou bleues est 39.

5. Théorèmes de Sylow

Théorème

Soit G un groupe d'ordre n . Soit p un nombre premier. On écrit $n = p^r m$ avec $p \nmid m$.

- ▶ Il existe un sous-groupe P d'ordre p^r . On appelle un tel groupe, un *p -Sylow* de G
- ▶ Soient P et Q deux *p -Sylow*, il existe $g \in G$ tel que $Q = gPg^{-1}$ (les p -Sylow sont conjugués deux à deux)
- ▶ Soit H un p -sous-groupe de G , alors H est contenu dans un p -Sylow
- ▶ Le nombre n_p de p -Sylow vérifie $n_p \mid m$ et $n_p \equiv 1 \pmod{p}$

Corollaire

Un groupe G d'ordre n possède un élément d'ordre p si et seulement si p divise n

Exemple

Soit G un groupe d'ordre pq avec $p < q$ premiers. Alors, $n_q \mid p$ et $n_q \equiv 1 \pmod{q}$ d'où $n_q = 1$. Il suit qu'il existe un unique q -Sylow Q qui est distingué. Soit P un p -Sylow, on a $P \cap Q = e$ et $G = PQ$ d'où $G \simeq \mathbb{Z}/p\mathbb{Z} \ltimes \mathbb{Z}/q\mathbb{Z}$.

Déterminer tous les groupes d'ordre 12 à isomorphisme près.

Soit G un groupe d'ordre 12.

1. Déterminer les valeurs possibles pour n_2 et n_3 .
2. Montrer que G est abélien si et seulement si $n_2 = n_3 = 1$.
 - 2.1 On suppose que G est abélien. Montrer que G contient au moins un élément d'ordre 6 ou 12.
 - 2.2 En déduire la structure de G dans le cas abélien.
3. On suppose à présent que G n'est pas abélien. Montrer que si $n_3 \neq 1$, alors on a $n_2 = 1$.
4. On suppose que $n_3 = 4$. On considère l'action de G sur les 3-Sylow par conjugaison.
 - 4.1 Montrer que le stabilisateur d'un 3-Sylow pour cette action est lui-même.
 - 4.2 En déduire que l'action est fidèle, puis que $G \simeq A_4$.
5. On suppose que $n_3 = 1$ et donc $n_2 = 3$. Montrer qu'on a dans ce cas
$$G \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z} \quad \text{ou} \quad G \simeq \mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2.$$
6. (Question subsidiaire.) Montrer $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2 \simeq D_{12}$.