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. (inversibilité) $\forall x \in G$, $\exists x' \in G$ 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)

$z^{-1}zx = z^{-1}zy \Rightarrow x = y$

e e

Définition

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

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

$x^{-n} = (x^{-1})^n$

$n \geq 1$

Additive

nx

$= x + \cdots + x$

$-nx$

$= (-x) + \cdots + (-x)$

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 $n \in \mathbb{Z}$, $(zxz^{-1})^n = zx^n z^{-1}$

$n \geq 1$ $zxz^{-1}zxz^{-1} \cdots zxz^{-1}$

Conjugué de x par z

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.

Exemple : $(\mathbb{R}^\times, \cdot)$ $2 \in \mathbb{R}^\times$, $2^n \neq 1 \Rightarrow 2$ 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*

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

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

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 un 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

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

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

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

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 $f : G_1 \to G_2$ 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 $\mathrm{Aut}(G)$.

Proposition

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

$$\mathrm{Im}(f) = \{f(x) : x \in G_1\} \qquad \text{image de } f$$

$$\mathrm{Ker}(f) = \{x \in G_1 \text{ tel que } f(x) = e_2\} \qquad \text{noyau de } f$$

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

Partie génératrice de $\mathrm{GL}_n(k)$.

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

Matrices de dilatations

$$I_n + \lambda E_{i,i} = \mathrm{diag}(1, \cdots, 1+\lambda, \cdots, 1) \qquad \text{avec } \lambda \neq -1$$

Matrices de transvections

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

Théorème

L'ensemble des matrices de dilatation et des matrices de transvection engendre le groupe (multiplicatif) $\mathrm{GL}_n(k)$.

Partie génératrice de $\mathrm{O}_n(k)$.

Matrice orthogonale. $M^t M = I_n \leftrightsquigarrow M$ 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 $\mapsto h - p$.

Théorème

L'ensemble des réflexions orthogonales engendre le groupe (multiplicatif) $\mathrm{O}_n(k)$ (qui est un sous-groupe de $\mathrm{GL}_n(k)$).

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 :

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

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 $x = gyg^{-1}$ qui donne les classes de conjugaison*

Théorème (Lagrange)

On a $\mathrm{card}(G/H) = \mathrm{card}(H\backslash G)$ *et* $|G| = \mathrm{card}(G/H)\,|H|$.
En particulier, si $|G|$ *est fini, l'ordre de tout sous-groupe de* G *et de tout élément de* G *divise* $|G|$.
On appelle $\mathrm{card}(G/H)$ *l'indice de* H *dans* G.

Remarque. La réciproque en fausse 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

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