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

$* : G \times G \to G$

Définition

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

1. (élément neutre) $\exists e \in G$ avec $x * e = e * x = x$ $\forall x \in G$
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 $x * x' = x' * x = e$

$(\mathbb{Z}, +)$ groupe $\qquad x' = x^{-1}$

$(\mathbb{R}^*, \times)$ groupe

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)*

$zx = yz \qquad x + y$

Résultat. Soient $x, y, z \in G$, $x\cancel{z} = y\cancel{z} \implies x = y$ (simplification) et $(xy)^{-1} = y^{-1}x^{-1}$ (inversion inverse l'ordre) not. mult.

Définition

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

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

$-n > 0$

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

$z x \cancel{z^{-1}} \cancel{z} x \cancel{z^{-1}} \cdots \cancel{z} x z^{-1}$ $= z x^n z^{-1}$

conjugaison de x par z

Définition

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

1 dans $(\mathbb{Z}, +)$ est d'ordre infini

1 dans $(\mathbb{R}^*, \times)$ est d'ordre 1

-1 ———————————————— 2

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.

$\Leftarrow$) si $n | t$, disons $t = nq$ alors $x^t = (x^n)^q = e^q = e$

$\Rightarrow$) div. euclidienne $t = nq + r$ avec $0 \leq r < n$

$x^t = (x^n)^q \cdot x^r$

Par hyp. $x^t = e$

$x^n = e \leadsto x^r = e$

donc $r = 0$

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

$x^n = x^m$ avec $n > m$ alors $x^{n-m} = e$

avec $n-m \geq 1$

Définition

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

$x = gxg^{-1}$ $\quad$ $g = x^{-1}gx$

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 :

  $xhx^{-1} = h$

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

  Note. $H \subseteq Z(G)$ ssi H est abélien. $\quad$ $Z_G(G) = Z(G)$

  H

- 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 $Z_H(G) \subseteq Z(G)$.

$S \neq \emptyset$ $\mathbb{Z} = \langle \{1\} \rangle = \langle 1 \rangle$

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.

$\rightarrow$ sous-groupes

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

ex

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

• sous-groupe

$\subseteq \langle S \rangle$

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

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

$$|\langle g \rangle| = \underline{\mathrm{ord}(g)}$$

Définition

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

G,

$G_1 \times G_2$ groupe neutre (e_1, e_2)

$(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2)$

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 $\boxed{G_1 \simeq G_2}$. Une isomorphisme entre G et lui-même est un automorphisme.

G_2

dans G_1 dans G_2

~~Bij(G)~~

Remarque

L'ensemble des automorphismes de G est un groupe pour la composition dénoté $\mathrm{Aut}(G)$.

Aut G

• neutre : id

• associativité

• inverse

$f(e_1) = e_2$ $f(x^{-1}) = f(x)^{-1}$

Proposition

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

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

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

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 $\mathrm{Ker}(f) = \{e_1\}$.

$x, y \in \mathrm{Ker}(f)$ $f(xy) = f(x)f(y) = e_2 e_2 = e_2$

Partie génératrice de $\mathrm{GL}_n(k)$ = groupe des matrices inv. $n \times n$ à coeff. dans $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$

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

Matrices de dilatations

$\mu \neq 0$

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

Matrices de transvections

i, j

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

Théorème

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

Partie génératrice de $\mathrm{O}_n(k)$ = groupe orthogonal

Matrice orthogonale: $\boxed{M^tM = I_n} \rightsquigarrow M$ inversible et $M^{-1} = {}^tM$.

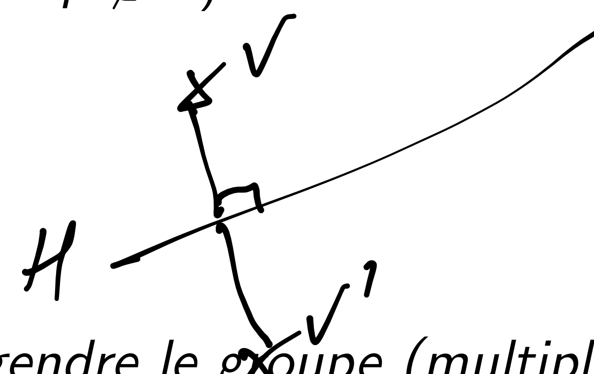
$M.{}^tM = I_n$

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 $x \mapsto h - p$.

$\mathbb{R}^2$

k^n hyp



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

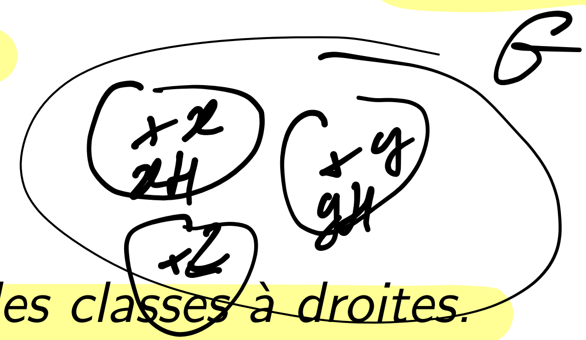
$A \xleftrightarrow{bij} gA$ $\quad a \mapsto ga$, $\quad g^{-1}x \leftarrow\!\shortmid x$ $\qquad Ag \xleftrightarrow{bij} gA$

Définition

Soit H sous-groupe de G. Relation d'équivalence sur G : $x \mapsto gxg^{-1}$

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

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*

G fini

$G = \bigcup_{g \in G \text{ repr.}} gH \Rightarrow |G| = \sum_{g \text{ repr.}} |gH|$

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*.*

$H = \langle g \rangle$

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).

indice H dans G

$[G:H] = (G:H) = |G|/|H|$

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

ordre $a \mid |(\mathbb{Z}/p\mathbb{Z})^*| = p-1$

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

$(\mathbb{Z}/n\mathbb{Z})^*$

$(a,n)=1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

$g \in \mathrm{Ker}\, s \iff gH = H \iff g \in H$

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 $H \lhd G$

$\{ghg^{-1} : h \in H\}$

$G \rhd H$

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

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

$g^{-1}Hg \subseteq H \Rightarrow H \subseteq gHg^{-1}$

Théorème

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

$ab \mapsto abH = aH\, bH$

$H = \mathrm{Ker} f$

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

$$G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f) \qquad (\textit{Théorème de factorisation})$$

gH

$\bar{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f) \qquad \bar{f}(gH) = f(g)$

Quelques applications du théorème de factorisation

1. Reconnaître les groupes suivants :
$$S_n/A_n, \quad \mathrm{O}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R}), \quad \mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}), \quad \mathbb{R}^\times/\mathbb{R}_+^\times.$$
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 $H \sqsubset K \sqsubset G \Longrightarrow H \sqsubset G$.
3. Démontrer que $H \sqsubset K \lhd G \Longrightarrow H \lhd G$.
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 :
$$G/Z(G) \simeq \mathrm{Int}(G).$$