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

$G \times G \xrightarrow{*} G$

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 $x * x' = x' * x = e$

sauf soustraction

neutre

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)*

$x^{-1} \longleftarrow x \cdot y = xy \qquad x + y \longrightarrow -x$

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

$(xy)(xy)^{-1}$

$(\mathbb{Z},+)$ $(\mathbb{R}^*,\cdot)$ $(\mathbb{Z}/n\mathbb{Z},\cdot)$ xy $y^{-1}x^{-1} = xx^{-1} = e$

e

Définition

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

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

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

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

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.

$-1 \in \mathbb{R}^*$ ordre 2

$1 \in \mathbb{Z}$ ordre infini

$i \in \mathbb{C}^*$ ordre 4

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.

$\Leftarrow$ $n | t$: il existe $q \in \mathbb{Z}$ $t = nq$ $\left(x^t = (x^n)^q = e^q = e \right)$

$\Rightarrow$ $x^t = e$: div. euclidienne de t par n

$\boxed{t = nq + r}$ avec $0 \leq r < n$

$x^r = x^{-nq} = e$

par minimalité de n, il suit $r = 0$ d'où $n | t$

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

$n \neq m$ $x^n = x^m \Rightarrow x^{n-m} = e$

$n > m$

Définition

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

Sous-groupes particuliers. → sous groupe = groupe

- Centre du groupe G : $Z(G) = \{x \in G : \forall g \in G, xg = gx\}$ $\quad g = x^{-1}gx$

  Note. $G = Z(G)$ ssi G est abélien.
- Pour H sous-groupe de G, le centralisateur de H :

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

  Note. $H \subseteq Z_H(G)$ ssi H est abélien. $\quad Z_G(G) = Z(G)$
- Pour H sous-groupe de G, le normalisateur de H : $\quad xHx^{-1} \subseteq H$

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

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

$\langle\{g\}\rangle$

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.

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

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

$\{g^n : n\in\mathbb{Z}\}$

$\langle S\rangle = \bigcap H$

$S\subseteq H$

H sous-gpe G

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 $|G|$.

$*$ dans G_1 $*$ dans G_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.

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

$f(x^n) = f(x)^n$

Remarque

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

$\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$ $\langle -1 \rangle = \{1, -1\}$

Proposition

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

$$\mathrm{Im}(f) = \{f(x) : x \in G_1\} \subseteq G_2 \qquad \textit{image de } f$$

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

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

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

k corps $k = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$

↳ matrices $n \times n$ inversibles (groupe pour mult.)

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

Matrices de dilatations

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

$\lambda \neq 0$

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 $\mathrm{O}_n(k)$ = sous-groupe des matrices orthogonales

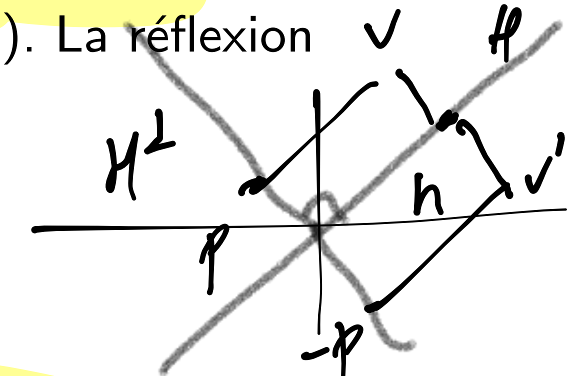
$GL_n(k)$

Matrice orthogonale. $M\underbrace{{}^tM}_{\text{transposée}} = I_n \leftrightsquigarrow M$ inversible et $M^{-1} = {}^tM$.

Ex. Montrer que c'est un sous-groupe

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) $\mathrm{O}_n(k)$ (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.

$\{xh : h \in H\} = \{yh : h \in H\} \iff \forall h \in H, \exists h' \in H$

Définition

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

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

$xh = yh'$

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

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

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

classe d'equivalence de 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 $\quad G = \bigsqcup C \Rightarrow |G| = \sum \mathrm{Card}\, C$

$C \in G/H$

$= \sum_{C \in G/H} |H| = \mathrm{card}(G/H)\cdot|H|$

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).

$m \geq 2$ entier a premier avec m

$a^{\varphi(m)} \equiv 1 \pmod m$

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

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

$\mathrm{ord}(\bar{a}) = n$ divise $p-1$

$\bar{a}^{p-1} = \bar{a}^{n.t} = (\bar{a}^{n})^{t} = \bar{1}$

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 $H \triangleleft G$

$g^{-1}Hg \subseteq H \iff H \subseteq gHg^{-1}$ $\forall g \in G$ $gH = Hg$

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

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

H distingué

$a'H$ $= a'b'H$

dépend de a et b

$= \{ah\}$

bien défini si $H \triangleleft G$

Théorème

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

$C, C' \in G/H$ notée

$H = eH$

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

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

distingué

$\varphi : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$

Quelques applications du théorème de factorisation

$\bar{g} \in G/\ker(f)$: $\varphi(\bar{g}) = f(g)$

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 $H \sqsubset K \triangleleft G \Longrightarrow H \triangleleft G$.
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 :

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

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 $G = HK$ $\Leftrightarrow \forall g \in G, \exists h \in H, k \in K \; g = hk$
- 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 $k \mapsto kH$

$G \to G/H$
$g \mapsto gH$

On note $G = H \rtimes K$.

$\times + \triangleleft$ $\quad H \triangleleft G$

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

$H \cap K = \{e\}$

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 $HK = G$
$H \times K \to G$ définit par

$H \times K \quad G$

$(h, k) \mapsto hk$

est un isomorphisme.

groupe

$(h, k) \cdot (h', k') = (hh', kk')$

G simple : seuls sous-groupes distingués sont $\{e\}$ et G

3. Quelques groupes particuliers

Lemme

$\exists g \in G,\ G = \langle g \rangle$

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.

ϕ morphisme • g ordre infini ϕ inj.

$\phi : \mathbb{Z} \to G$, $t \mapsto g^t$ $\quad \mathrm{Im}\,\phi = G$

• g d'ordre n $\quad \mathrm{Ker}\,\phi = n\mathbb{Z}$

Proposition

Soit $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$. L'ordre de $\bar{m}$ est $n/\mathrm{PGCD}(m,n)$ 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

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

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

$\varphi(p^e) = p^{e-1}(p-1)$, p premier, $e \geq 1$

Théorème (Théorème des restes chinois)

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

$\hookrightarrow \varphi(nm) = \varphi(n) \times \varphi(m)$

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

p premier $(\mathbb{Z}/p\mathbb{Z})^*$ cyclique | p premier impair $e \geq 1$ $(\mathbb{Z}/p^e\mathbb{Z})^*$ cyclique

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 $\mathrm{Aut}((\mathbb{Z}/22\mathbb{Z})^*)$ 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 $\mathrm{Aut}((\mathbb{Z}/22\mathbb{Z})^*)$ et en déduire que $\mathrm{Aut}((\mathbb{Z}/22\mathbb{Z})^*)$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Définition

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

Exemple

Les permutations peuvent s'écrire de deux manières essentiellement

image

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

$$(1,4,5)(2,3)(6,8)\cancel{(7)} \quad \text{(produit de cycles disjoints)}$$

Remarques

$(4,5,1) = (5,1,4) \neq (5,4,1)$

- *La multiplication se fait de droite à gauche* $(1,2)(2,3) = (1,2,3)$

  $1 \leftarrow 2 \leftarrow 3$
- *On a* $(a_1, a_2, \ldots, a_s) = (a_2, a_3, \ldots, a_s, a_1) = \cdots = (a_s, a_1, \ldots, a_{s-1})$

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

Résultat. Les transpositions engendrent S_n.

$(1,2)(2,3)(3,4) = (1,2,3,4)$

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.

$\varepsilon \quad n! = S_n/A_n \simeq \{\pm 1\}$ $=2$

Proposition

Il existe un unique morphisme $\mathrm{sign} : S_n \to \{\pm 1\}$ non trivial. On l'appelle la signature. Soit c un ℓ-cycle, on a $\mathrm{sign}(c) = (-1)^{\ell+1}$.
Une permutation π est paire si $\mathrm{sign}(\pi) = 1$ et impaire si $\mathrm{sign}(\pi) = -1$.
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.

groupe simple abélien : $\mathbb{Z}/p\mathbb{Z}$ p premier.

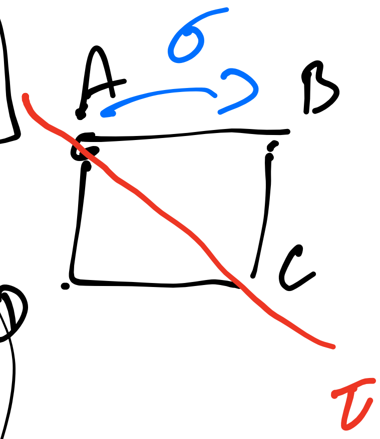
Soit $n \geq 3$. Le groupe diédral D_{2n} est le groupe des isométries du plan qui fixe un polygone régulier à n côtés.

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

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

σ d'ordre n $\quad$ τ d'ordre 2 $\quad$ $\tau\sigma\tau^{-1}$



On a alors

car $\tau = \tau^{-1}$

- 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

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

$\tau(\sigma(A)) = \sigma^{-1}(A)$

$\to$ D_{2n} possède n élts d'ordre 2

1. tous distincts

2. $g \in \langle \sigma, \tau \rangle$ alors $g =$

$\to$ $\tau\sigma = \sigma^{-1}\tau$

4. Actions de groupe

Définition

Une action du groupe G sur un ensemble X est la donnée d'un morphisme $\Phi : G \to \mathrm{Bij}(X)$ ($=$ 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

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

$\in X$

$\Phi(g) \in \mathrm{Bij}(X)$

$\hookrightarrow x \mapsto g \cdot x$

X

Définition

Pour $x \in X$, on pose $G \cdot x$

- $O(x) = \Omega_x = \{g \cdot x : g \in G\}$ 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)

$g \in \text{Noyau} \iff \forall x \in X$ $g \cdot x = x$

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

On note X/G l'ensemble des orbites de X. $\leftarrow$ forment une partition de X

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

L'action est fidèle si le noyau est trivial.

$X = \bigsqcup_{\Omega \in X/G} \Omega$

Lemme

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

$\bar{g} \in G/K \quad \bar{g} \cdot x = g \cdot x$

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

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

$G \to \Omega_x$

$g \mapsto g \cdot x$

Soit $x \in X$, on a

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

stab.

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

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