Groupes

Rappels : relations d'équivalence et ensembles quotients

Définition

Soit X un ensemble. Une *relation d'équivalence* sur X est une relation binaire $\mathcal{R}$ sur X vérifiant les propriétés suivantes :

- $(\forall x \in X)\, x\mathcal{R}x$ (réflexivité) ;
- $(\forall x, y \in X)\, x\mathcal{R}y \Rightarrow y\mathcal{R}x$ (symétrie) ;
- $(\forall x, y, z \in X)\, (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$ (transitivité).

La *classe d'équivalence* de $x \in X$ est alors $[x] := \{y \in X\,;\, x\mathcal{R}y\}$.
Les classes d'équivalence forment une partition de X.
L'*ensemble quotient* $X/\mathcal{R}$ est la partie de $\mathscr{P}(X)$ constituée par les classes d'équivalences. Si $A \in X/\mathcal{R}$, on a $A = [x]$ pour tout $x \in A$: un tel élément x s'appelle un *représentant* de A.

Rappels : relations d'équivalence et ensembles quotients

Exemple

Soit $f : X \to Y$ une application. On définit une relation d'équivalence $\mathcal{R}_f$ sur X en posant $x_1 \mathcal{R}_f x_2 \Leftrightarrow f(x_1) = f(x_2)$. Les classes d'équivalence sont les préimages non vides des singletons.

Définition

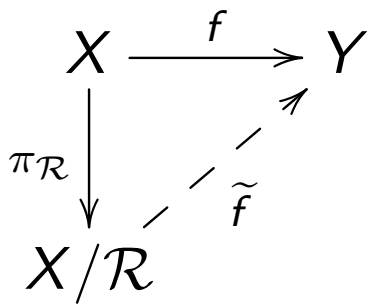
Si $\mathcal{R}$ est une relation d'équivalence sur un ensemble X, on dispose de la *surjection canonique*

$$\begin{aligned} \pi_{\mathcal{R}} : X &\to X/\mathcal{R} \\ x &\mapsto [x]. \end{aligned}$$

Un *système (complet) de représentants* est une partie $T \subset X$ telle que la restriction de $\pi_{\mathcal{R}}$ à T induise une bijection $T \xrightarrow{\sim} X/\mathcal{R}$. Cela signifie que pour tout $A \in X/\mathcal{R}$, il existe un unique $t \in T$ tel que $A = [t]$, *i.e.* tel que t soit un représentant de A.

Proposition - Propriété universelle

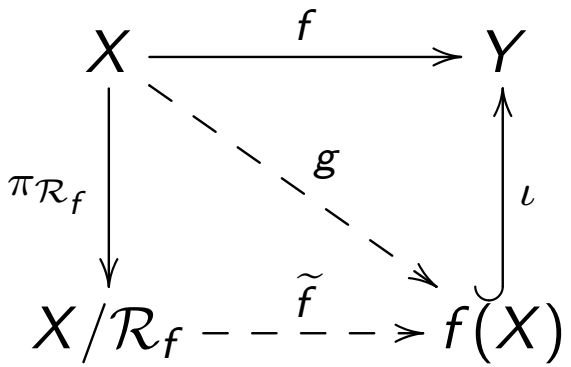
Soient $\mathcal{R}$ une relation d'équivalence sur un ensemble X et $f : X \to Y$ une application telle que $x_1 \mathcal{R} x_2 \Rightarrow f(x_1) = f(x_2)$. Alors il existe une unique application $\widetilde{f} : X/\mathcal{R} \to Y$ telle que $f = \widetilde{f} \circ \pi_{\mathcal{R}}$.



Si $A \in X/\mathcal{R}$ et $x \in A$, on a nécessairement $\widetilde{f}(A) = f(x)$.

Corollaire - Décomposition canonique d'une application

Soit $f : X \to Y$ une application. Il existe une unique application $\widetilde{f} : X/\mathcal{R}_f \to f(X)$ telle que $f = \iota \circ \widetilde{f} \circ \pi_{\mathcal{R}_f}$ où $\iota : f(X) \hookrightarrow Y$ est l'inclusion. L'application $\widetilde{f}$ est bijective.



Définition

Un *groupe* est un couple $(G, *)$ où G est un ensemble, $*\colon G \times G \to G$ une loi de composition interne, vérifiant les conditions suivantes :

- on a $(x * y) * z = x * (y * z)$ pour tous $x, y, z \in G$ (associativité) ;
- il existe un élément $e \in G$ tel que $e * x = x * e = x$ pour tout $x \in G$ (élément neutre) ;
- pour tout $x \in G$, il existe un élément $x' \in G$ tel que $x * x' = x' * x = e$ (inverse).

On dit que G est *abélien* (ou *commutatif*) lorsque $x * y = y * x$ pour tous $x, y \in G$.

Rappels : groupes

Définition

(1) un *morphisme* entre deux groupes $(G, *)$ et $(G', \bullet)$ est une application $f : G \to G'$ telle que $f(x * y) = f(x) \bullet f(y)$ pour tous $x, y \in G$ (on a alors $f(x^{-1}) = f(x)^{-1}$ pour tout $x \in G$, et $f(e_G) = e_{G'}$) ;
(2) un sous-groupe $H \leq G$ est une partie $H \subset G$ telle que l'inclusion soit un morphisme de groupes. On dit qu'on sous-groupe $H \leq G$ est *distingué* lorsque $(\forall x \in G)\, xH = Hx$;
(3) Le *noyau* (resp. l'*image*) d'un morphisme de groupes $f : G \to G'$ est $\mathrm{Ker}(f) = f^{-1}(e_{G'})$ (resp. $f(G)$). C'est un sous-groupe distingué de G (resp. un sous-groupe de G').

Exemple

Les sous-groupes de $\mathbb{Z}$ sont les parties de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Rappels : groupes

Définition

Notion de sous-groupe engendré par une partie.

Définition

L'*ordre* d'un groupe G est son cardinal. Si $g \in G$, l'*ordre* de g est l'ordre du sous-groupe engendré $\langle g \rangle = \{g^n \, ; \, n \in \mathbb{Z}\}$. C'est aussi le plus petit entier $n \in \mathbb{N}_{>0}$ tel que $g^n = e$, ou $+\infty$ si un tel entier n'existe pas.

Définition - Classes modulo un sous-groupe

Soient G un groupe et $H \leq G$ un sous-groupe. On définit une relation d'équivalence sur G en posant $g_1 \mathcal{R}_H g_2 \Leftrightarrow g_1^{-1} g_2 \in H$. Les classes d'équivalence sont les *classes à gauche* modulo H : ce sont les parties de la forme gH. On note G/H l'*ensemble* de ces classes à gauche. On pose $(G : H) = \#(G/H)$ (*l'indice* de H dans G).

Rappels : groupes

Théorème de Lagrange

Si G est un groupe fini et H un sous-groupe. On a $\#G = (G : H)\#H$ d'où $\#H \mid \#G$. En particulier, l'ordre d'un élément $g \in G$ divise $\#G$.

Proposition

Si H est un sous-groupe distingué, l'ensemble G/H est muni d'une unique structure de groupe, pour laquelle la surjection canonique $G \to G/H$ est un morphisme de groupes.

Si $g_1, g_2, g \in G$, on a

$$(g_1 H)(g_2 H) = g_1 g_2 H$$

$$(gH)^{-1} = g^{-1} H$$

(l'élément neutre est la classe triviale H).

Rappels : groupes

Proposition

Soit G un groupe. Les relations d'équivalence sur G qui sont compatibles avec la loi de groupe sont les relations modulo un sous-groupe distingué.

Remarque

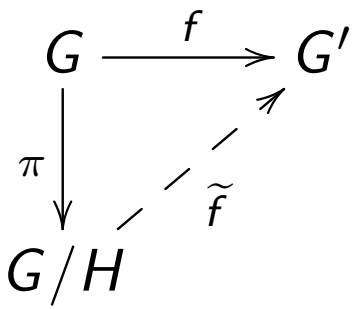
Dans la pratique, on note $\overline{g}$ la classe gH, lorsque cela ne prête pas à confusion.

Exemple

Si $n \in \mathbb{Z}_{\geq 0}$, on dispose du groupe quotient $\mathbb{Z}/n\mathbb{Z}$.

Proposition - propriété universelle

Soient $f : G \to G'$ un morphisme de groupes et $H \leq G$ un sous-groupe distingué tel que $H \subset \mathrm{Ker}(f)$. Alors il existe un unique morphisme de groupes $\widetilde{f} : G/H \to G'$ tel que $f = \widetilde{f} \circ \pi$, où $\pi : G \to G/H$ est la surjection canonique.



Exemple

Si $f : G \to G'$ est un morphisme de groupes, alors f induit un isomorphisme $G/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Im}(f)$.

Théorèmes d'isomorphisme

Soit G un groupe.

(1) Si $H \leq G$ et $N \lhd G$, alors $HN = \{hn\}_{\substack{h\in H\\ n\in N}}$ est un sous-groupe de G, $N \cap H \lhd H$ et on a un isomorphisme

$$H/(N \cap H) \xrightarrow{\sim} HN/N.$$

(2) Soient H et K deux sous-groupes distingués de G. Si $K \leq H$, alors $H/K \lhd G/K$ et on a un isomorphisme

$$(G/K)/(H/K) \xrightarrow{\sim} G/H.$$

Proposition

Soit $n \in \mathbb{N}_{>0}$. Pour tout diviseur d de n, il existe un et un seul sous-groupe d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$: c'est le sous-groupe engendré par $\frac{n}{d}$.

Le groupe symétrique : généralités

Définition

Si E est un ensemble, on note $\mathfrak{S}_E$ l'ensemble des *permutations* de E, *i.e.* des bijections de E dans lui-même. C'est un groupe pour la composition. Si $n \in \mathbb{N}_{>0}$, on note $\mathfrak{S}_n$ le groupe des permutations de $\{1, \ldots, n\}$.

Dans tout ce qui suit, on fixe $n \in \mathbb{N}_{>0}$.

Proposition

On a $\#\mathfrak{S}_n = n!$.

Le groupe symétrique : généralités

Définition

(1) Si $\sigma \in \mathfrak{S}_n$, on note $\mathrm{Fix}(\sigma) = \{i \in \{1, \dots, n\} \,;\, \sigma(i) = i\}$ l'ensemble des points fixes. L'ensemble $\mathrm{supp}(\sigma) := \{1, \dots, n\} \setminus \mathrm{Fix}(\sigma)$ s'appelle le *support* de σ.

(2) Soient $\ell \in \mathbb{N}_{>1}$ et $i_1, \dots, i_\ell$ des éléments distincts de $\{1, \dots, n\}$. On note $(i_1, \dots, i_\ell)$ l'élément de $\mathfrak{S}_n$ qui envoie i_ℓ sur i_1, i_k sur i_{k+1} pour tout $k \in \{1, \dots, \ell - 1\}$ et laisse fixe tous les éléments de $\{1 \dots, n\} \setminus \{i_1, \dots, i_\ell\}$ (on a donc $\mathrm{supp}(i_1, \dots, i_\ell) = \{i_1, \dots, i_\ell\}$. Une permutation de ce type est appelée *cycle* de longueur ℓ ou ℓ-*cycle*. Un 2-cycle s'appelle une *transposition*.

Remarque

(1) Un ℓ-cycle est d'ordre ℓ.

(2) Il y a $\frac{n(n-1)\cdots(n-\ell+1)}{\ell} = \binom{n}{\ell}(\ell - 1)!$ cycles de longueur ℓ.

Le groupe symétrique : généralités

Lemme

Si $\text{supp}(\sigma_1) \cap \text{supp}(\sigma_2) = \varnothing$, alors $\text{supp}(\sigma_1\sigma_2) = \text{supp}(\sigma_1) \cup \text{supp}(\sigma_2)$, σ_1 et σ_2 commutent et $\sigma_1\sigma_2 = \text{Id} \Rightarrow \sigma_1 = \sigma_2 = \text{Id}$.

Théorème (décomposition en produit de cycles à supports disjoints)

Soit $\sigma \in \mathfrak{S}_n$. Il existe $c_1, \ldots, c_r \in \mathfrak{S}_n$ des cycles à supports deux à deux disjoints tels que $\sigma = c_1 \cdots c_r$. Une telle décomposition est unique à l'ordre des facteurs près.

Corollaire

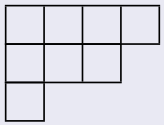
Le groupe $\mathfrak{S}_n$ admet les parties génératrices suivantes :

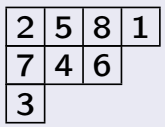
- les transpositions ;
- $\{(1, i)\}_{2 \leq i \leq n}$;
- $\{(i, i+1)\}_{1 \leq i \leq n-1}$;
- $\{(1, 2), (1, 2, \ldots, n)\}$.

Le groupe symétrique : généralités

Définition

(1) Le *type* de $\sigma \in \mathfrak{S}_n$ est la suite $\underline{\ell} = (\ell_1, \ldots, \ell_r)$ (ordonnée dans l'ordre décroissant) des longueurs des cycles apparaissant dans la décomposition de σ en produit de cycles à support disjoints, auxquelles on adjoint une suite de 1 correspondant aux points fixes. C'est une *partition* de n (*i.e.* on a $\ell_1 + \cdots + \ell_r = n$).

(2) L'ensemble des partitions de n est en bijection avec les *diagrammes de Young*. Par exemple, $(4,3,1) \leftrightarrow$  .

(3) Un *tableau de Young* est un diagramme de Young rempli avec les entiers de 1 à n. Un tel tableau correspond à une décomposition d'un élément de $\mathfrak{S}_n$ en produit de cycles à supports disjoints. Par exemple, $(2,5,8,1)(7,4,6) \leftrightarrow$  .

Le *tableau de Young standard* (de type $\underline{\ell}$) est celui dont les cases sont remplies dans l'ordre, par exemple  .

Lemme

Soient $c = (i_1, \ldots, i_\ell)$ un cycle de longueur ℓ et $\sigma \in \mathfrak{S}_n$. On a

$$\sigma c \sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_\ell)).$$

Théorème

Deux éléments de $\mathfrak{S}_n$ sont conjugués dans $\mathfrak{S}_n$ si et seulement s'ils ont même type.

Théorème

Si $n \geq 3$, le centre de $\mathfrak{S}_n$ est trivial.

Exercice

Montrer que $\mathfrak{S}_{11}$ contient un élément d'ordre 24, mais pas d'élément d'ordre 22.

Le groupe symétrique : signature et groupe alterné

Définition

Si $\sigma \in \mathfrak{S}_n$, on pose $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$.

Remarque

Un élément $\sigma \in \mathfrak{S}_n$ permute les parties à 2 éléments de $\{1, \ldots, n\}$. Cela implique que $\varepsilon(\sigma) \in \{\pm 1\}$.

Lemme

Si $c \in \mathfrak{S}_n$ est un ℓ-cycle, on a $\varepsilon(\tau) = (-1)^{\ell - 1}$. En particulier, on $\varepsilon(\tau) = -1$ pour toute transposition $\tau \in \mathfrak{S}_n$.

Théorème

L'application ε définit un morphisme de groupes $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$. Il est surjectif lorsque $n \geq 2$.

Le groupe symétrique : signature et groupe alterné

Définition

Le *groupe alterné* est $\mathfrak{A}_n = \mathrm{Ker}(\varepsilon)$. C'est un sous-groupe distingué de $\mathfrak{S}_n$, d'indice 2 lorsque $n \geq 2$.

Proposition

Le groupe $\mathfrak{A}_n$ admet les parties génératrices suivantes :

- $\{(1,i)(1,j)\}_{2\leq i<j\leq n}$;
- $\{(1,2,i)\}_{3\leq i\leq n}$ (et donc par les 3-cycles) ;
- $\{\sigma^2\}_{\sigma\in\mathfrak{S}_n}$.

Remarque

Les classes de conjugaison de $\mathfrak{A}_n$ sont un peu plus compliquées que celles de $\mathfrak{S}_n$: deux permutations paires de même type peuvent ne pas être conjuguées dans $\mathfrak{A}_n$.

Les classes de conjugaison de $\mathfrak{S}_5$.

partition	représentant	cardinal de la classe de conjugaison
$(1,1,1,1,1)$	Id	1
$(2,1,1,1)$	$(1,2)$	$\binom{5}{2} = 10$
$(2,2,1)$	$(1,2)(3,4)$	$\frac{1}{2}\binom{5}{2}\binom{3}{2} = 15$
$(3,1,1)$	$(1,2,3)$	$\frac{5\times4\times3}{3} = 20$
$(3,2)$	$(1,2,3)(4,5)$	20
$(4,1)$	$(1,2,3,4)$	$\frac{5\times4\times3\times2}{4} = 30$
(5)	$(1,2,3,4,5)$	$\frac{5!}{5} = 4! = 24$

Le groupe symétrique : signature et groupe alterné

Les classes de conjugaison de $\mathfrak{A}_5$.

partition	représentant	cardinal de la classe de conjugaison
$(1,1,1,1,1)$	Id	1
$(2,2,1)$	$(1,2)(3,4)$	15
$(3,1,1)$	$(1,2,3)$	20
(5)	$(1,2,3,4,5)$	deux classes de 12 éléments

Définition

Un groupe G est dit *simple* lorsque ses seuls sous-groupes distingués sont $\{e\}$ et G.

Théorème

Si $n \geq 5$, le groupe $\mathfrak{A}_n$ est simple.

Remarque

Les groupes $\mathfrak{A}_2$ et $\mathfrak{A}_3$ sont simples, mais pas $\mathfrak{A}_4$, qui contient le groupe de Klein des double transpositions.

Corollaire

Si $n \geq 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.

Exercice

Déterminer tous les morphismes de groupes $\mathfrak{S}_n \to \mathbb{C}^\times$.

Exercice

Existe-t-il un morphisme surjectif $\mathfrak{S}_n \to \mathfrak{S}_{n-1}$?

Produits semi-directs (internes)

Soient G un groupe, N et H deux sous-groupes de G.

Lemme

Si $N \lhd G$, l'ensemble $NH := \{xy\}_{\substack{x \in N \\ y \in H}}$ est un sous-groupe de G.

Définition

On dit que G est *produit semi-direct interne* de H par N lorsque

- $N \lhd G$;
- $N \cap H = \{e\}$;
- $NH = G$.

On note alors $G = N \rtimes H$.

Produits semi-directs (internes)

Supposons que G soit produit semi-direct interne de H par N. Pour tout $y \in H$, on dispose de l'automorphisme $\varphi_y \in \mathrm{Aut}(N)$ défini par $\varphi_y(x) = yxy^{-1}$.

Proposition

(1) Pour tout $g \in G$, il existe $x \in N$ et $y \in H$ uniques tels que $g = xy$.

(2) Si $g_1 = x_1y_1, g_2 = x_2y_2 \in G$ avec $x_1, x_2 \in N$ et $y_1, y_2 \in H$, on a

$$g_1g_2 = (x_1\varphi_{y_1}(x_2))(y_1y_2).$$

(3) L'application $\varphi\colon H \to \mathrm{Aut}(N)$ est un morphisme de groupes.

Produits semi-directs (internes)

Remarque

Supposons G fini, que $N \lhd G$ et $N \cap H = \{e\}$. Alors $\#N\#H = \#G$ si et seulement si $NH = G$.

Exemples

(1) $\mathfrak{S}_3 = \mathfrak{A}_3 \rtimes \langle (1,2) \rangle$.

(2) Exemple crucial : le groupe diédral d'ordre $2n$

(3) Notons V le groupe de Klein : le sous-groupe de $\mathfrak{A}_4$ constitué de Id et des trois double-transpositions. On a $V \simeq (\mathbb{Z}/2\mathbb{Z})^2$ et $V \lhd \mathfrak{A}_4$. Soient c un 3-cycle (par exemple $c = (1,2,3)$) et $H = \langle c \rangle \simeq \mathbb{Z}/3\mathbb{Z}$. Alors $\mathfrak{A}_4 = V \rtimes H$.

(4) Soit $(\mathscr{E}, E)$ un espace affine. Le choix d'un point $\Omega \in \mathscr{E}$ perment de vectorialiser $\mathscr{E}$ (*i.e.* fournit la bijection $\mathscr{E} \xrightarrow{\sim} E$; $M \mapsto \overrightarrow{\Omega M}$). Si $H_\Omega = \mathrm{Fix}(\Omega) \leq \mathrm{GA}(\mathscr{E})$, on a $H_\Omega \xrightarrow{\sim} \mathrm{GL}(E)$ et $\mathrm{GA}(\mathscr{E}) = \mathrm{T}(\mathscr{E}) \rtimes H_\Omega$.

Produits semi-directs (externes)

Soient N et H deux groupes et

$$\varphi \colon H \to \mathrm{Aut}(N)$$
$$y \mapsto \varphi_y$$

un morphisme de groupes.

Définition

Le *produit semi-direct (externe)* de H par N (relativement à φ) est le groupe $N \rtimes_\varphi H$ dont l'ensemble sous-jacent est $N \times H$ (produit direct d'ensembles) et la loi est donnée par

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 \varphi_{y_1}(x_2), y_1 y_2).$$

Proposition

Ce qui précède définit bien un groupe, d'élément neutre (e_N, e_H).

Produits semi-directs (externes)

Remarque

Il est facile de vérifier que $N \rtimes_\varphi H$ est produit semi-direct interne de $\{e_N\} \times H$ par $N \times \{e_H\}$. Pour $x \in N$ et $y \in H$, on a alors

$$(\varphi_y(x), e_H) = (e_N, y) \cdot (x, e_H) \cdot (e_N, y)^{-1}.$$

Proposition

Le produit semi-direct $N \rtimes_\varphi H$ est direct (*i.e.* égal au produit cartésien $N \times H$ des groupes N et H) si et seulement si $\varphi \colon H \to \mathrm{Aut}(N)$ est trivial.

Exemples

(1) Pour tout $n \in \mathbb{N}_{>0}$, on a $D_{2n} \simeq (\mathbb{Z}/n\mathbb{Z}) \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z})$ où $\varphi(\bar{1})$ est la multiplication par -1 dans $\mathbb{Z}/n\mathbb{Z}$.

(3) Si $n \in \mathbb{N}_{\geq 2}$ et $\tau \in \mathfrak{S}_n$ une transposition, on a $\mathfrak{S}_n \simeq \mathfrak{A}_n \rtimes_\varphi \{\pm 1\}$, où $\varphi(-1)$ est la conjugaison par τ.

Actions de groupes : rappels

Définition

Une *action* (à gauche) de G sur X est la donnée d'une application

$$*\colon G \times X \to X$$

ayant les propriétés suivantes :

(i) $(\forall g_1, g_2 \in G)\,(\forall x \in X)\; g_1 * (g_2 * x) = (g_1 g_2) * x$;

(ii) $(\forall x \in X)\; e * x = x$.

On dit aussi que G agit sur X.

Remarque

Notion d'action à droite.

Actions de groupes : rappels

Si $*\colon G \times X \to X$ est une action, et si $g \in G$, on dispose de

$$\begin{aligned} \rho(g)\colon X &\to X \\ x &\mapsto g * x \end{aligned}$$

Proposition

L'application $\rho\colon G \to \mathfrak{S}_X$ est un morphisme de groupes.

Si $g \in G$ et $x \in X$, on a $g * x = \rho(g)(x)$.
Réciproquement, si on se donne un morphisme de groupes $f\colon G \to \mathfrak{S}_X$, on définit une action de G sur X en posant $g * x = f(g)(x)$ pour tout $g \in G$ et $x \in X$.

Proposition

La donnée d'une action de G sur X équivaut à celle d'un morphisme de groupes $G \to \mathfrak{S}_X$.

Exemples

(1) Le groupe G agit sur lui-même par translation à gauche : l'action est donnée par $g * x = gx$ pour tous $g, x \in G$. L'action par translation à droite est donnée par $(x, g) \mapsto xg^{-1}$.
(2) Plus généralement, si $H \leq G$ est un sous-groupe, on fait agir G sur G/H par translation à gauche en posant $g * (\gamma H) = g\gamma H = \{gx\}_{x \in \gamma H}$.
(3) Le groupe $\mathfrak{S}_X$ agit sur X de la façon naturelle, par $\sigma * x = \sigma(x)$. Le morphisme de groupes associé n'est autre que l'identité de $\mathfrak{S}_X$. Cas particulier où $X = \{1, \ldots, n\}$.
(4) Tout groupe agit sur lui-même par conjugaison (en posant $g * x = gxg^{-1}$ pour tout $g, x \in G$).
(5) Exemples en algèbre linéaire et en géométrie.

Actions de groupes : rappels

Définition

Soit G un groupe agissant sur un ensemble X.

(1) L'*orbite* de $x \in X$ est l'ensemble $G * x = \{g * x\}_{g \in G}$, c'est une partie de X, on la note $\mathrm{orb}(x)$.

(2) Le *stabilisateur* de $x \in X$ est

$$\mathrm{stab}_G(x) = \{g \in G \,;\, g * x = x\}.$$

C'est un sous-groupe de G.

(3) On dit que l'action est *fidèle* lorsque le morphisme associé $\rho \colon G \to \mathfrak{S}_X$ est injectif.

(4) On dit que l'action est *libre* lorsque pour tout $x \in X$, on a $g \cdot x = x \Rightarrow g = e$.

(5) On dit que l'action est *transitive* s'il n'y a qu'une seule orbite.

Actions de groupes : rappels

Remarque

(1) Si $x_1, x_2 \in X$, on pose $x_1 \sim x_2$ lorsqu'il existe $g \in G$ tel que $x_2 = g * x_1$. Cela définit une relation d'équivalence sur X, dont les classes d'équivalence ne sont autres que les orbites. En particulier, les orbites forment une partition de X.
(2) L'action induite de G sur chaque orbite est transitive.

Exemples - définitions

(1) Si H est un sous-groupe de G, l'action de G sur G/H par translation à gauche est transitive.
(2) Si G agit sur lui-même par conjugaison, l'orbite de x s'appelle la *classe de conjugaison* de x, son stabilisateur est le sous-groupe $C_G(x)$ des éléments de G qui commutent à x, le *centralisateur* de x.
(3) Lorsque G agit sur l'ensemble de ses sous-groupes par conjugaison, le stabilisateur d'un sous-groupe $H \leq G$ s'appelle le *normalisateur* de H et se note $\mathrm{N}_G(H)$.

Théorème de Cayley

L'action de G sur lui-même par translation à gauche est fidèle. Elle permet en particulier de voir G comme un sous-groupe de $\mathfrak{S}_G \simeq \mathfrak{S}_n$, où $n = \#G$.

Lemme

Si $g \in G$ et $x \in X$, alors

$$\mathrm{stab}_G(g * x) = g\,\mathrm{stab}_G(x)g^{-1}.$$

Théorème (relation orbite-stabilisateur)

Si $x \in X$, l'application

$$\begin{aligned} G/\mathrm{stab}_G(x) &\to \mathrm{orb}_X(x) \\ \overline{g} &\mapsto g \cdot x \end{aligned}$$

est bijective.

Corollaire

Si G est fini et $x \in X$, on a $\#G = \#\mathrm{orb}_X(x)\#\mathrm{stab}_G(x)$, en particulier l'entier $\#\mathrm{orb}_X(x) = (G : \mathrm{stab}_G(x))$ divise $\#G$.

Proposition (équation aux classes)

Supposons X fini. Si $\{x_1, \ldots, x_r\}$ est un système complet de représentants des orbites de X, on a

$$\#X = \sum_{i=1}^{r} \#\,\mathrm{orb}_X(x_i) = \sum_{i=1}^{r} (G : \mathrm{stab}_G(x_i)).$$

Corollaire

Si G est un p-groupe et X est fini, on a $\#X \equiv \#X^G \mod p\mathbb{Z}$ (où X^G désigne l'ensemble des points fixes).

Corollaire

Le centre d'un p-groupe est non trivial (par récurrence, pour tout $k \in \mathbb{N}$ tel que $p^k \mid \#G$, le p-groupe contient un sous-groupe distingué d'ordre p^k).

Proposition (formule de Burnside)

Supposons G et X finis. Pour tout $x \in X$, posons $\mathrm{Fix}(g) = \{x \in X \,;\, g \cdot x = x\}$ (les points fixes de g dans X). Le nombre d'orbites dans X est $\frac{1}{\#G} \sum_{g \in G} \#\,\mathrm{Fix}(g)$ (c'est le nombre moyen de points fixes).

Quelques exemples d'utilisation des actions de groupes.

Proposition

Soient G un groupe et $H \leq G$ un sous-groupe d'indice n. Il existe un sous-groupe *distingué* N de G tel que $N \subset H$ et $(G : N) \mid n!$.

Proposition

Soient G un groupe fini, $H \leq G$ un sous-groupe et p le plus petit diviseur premier de $\#G$. Si $(G : H) = p$, alors $H \lhd G$.

Exercice

Soit G un groupe d'ordre 33 agissant sur un ensemble de cardinal 19. Montrer qu'il y a au moins un point fixe.

Proposition

Soit p un nombre premier. Tout groupe de cardinal p^2 est abélien.

Remarque

Soit $G = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \; ; \; x, y, z \in \mathbb{Z}/p\mathbb{Z} \right\} \leq \mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z})$ le sous-groupe des matrices triangulaires supérieures unipotentes. Il est non abélien de cardinal p^3.

Théorème de Cauchy

Soient G un groupe fini et p un nombre premier divisant $\#G$. Alors G contient un élément d'ordre p.

Définition

Si G est un groupe fini, un *p-sous-groupe de Sylow* (ou simplement p-Sylow) de G est un sous-groupe de G d'ordre $p^{v_p(\#G)}$.
On note $\mathrm{Syl}_p(G)$ l'ensemble des p-Sylow de G et on pose $n_p(G) = \#\,\mathrm{Syl}_p(G)$.

Remarque

Si p ne divise pas $\#G$, alors $\{e\}$ est l'unique p-Sylow de G.

Théorèmes de Sylow

(i) $n_p \equiv 1 \mod p\mathbb{Z}$, en particulier $\mathrm{Syl}_p(G)$ n'est pas vide ;

(ii) le groupe G agit transitivement par conjugaison sur $\mathrm{Syl}_p(G)$ (les p-Sylow de G sont conjugués), en particulier $n_p(G) \mid \#G$.

Lemme

Si $r \in \mathbb{N}$ et $m \in \mathbb{N}_{>0}$, on a $\binom{p^r m}{p^r} \equiv m \mod p$.

Lemme

Soit H un p-sous-groupe de G et S_0 un p-Sylow de G. Alors H est inclus dans un conjugué de S_0.

Corollaire

Le groupe G admet un unique p-Sylow, si et seulement si ce dernier est distingué dans G.

Exercice

Soient G un groupe fini, $H \leq G$ un sous-groupe et p un nombre premier. Soit Q un p-Sylow de H. Montrer qu'il existe un p-Sylow S de G tel que $Q = S \cap H$.

Quelques exemples d'utilisation des théorèmes de Sylow.

Proposition

Tout groupe d'ordre 77 est cyclique.

Proposition

Il n'existe pas de groupe simple d'ordre 945.

Exercice

Déterminer le nombre de p-Sylow du groupe symétrique $\mathfrak{S}_p$.

Exercice

Un groupe d'ordre 300 n'est jamais simple.