Groupes

I Rappel sur les groupes

I.1 Définition

Définition

On dit que $(G, \cdot)$ est un groupe lorsque :
- $\cdot$ est une loi de composition interne
- $\cdot$ est associative
- G possède un neutre e_G pour $\cdot$
- Tout élément x de G possède un inverse x^{-1} tel que $x \cdot x^{-1} = x^{-1} \cdot x = e_G$

Si la loi $\cdot$ est commutative, on dira que $(G, \cdot)$ est abélien.

Notation. On notera parfois le neutre e, ou 1, ou encore 1_G. On utilisera parfois $\times$ à la place de $\cdot$, voire même $+$ dans le cas des groupes abéliens. Si $n \in \mathbb{N}$, on notera $x^n = x \times \cdots \times x$ par analogie avec les puissances de réels.

I.2 Quelques groupes de référence

- Les principaux groupes numériques additifs sont $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, et $(\mathbb{Z}/n\mathbb{Z}, +)$.
- Les principaux groupes numériques additifs sont $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}, \times)$ le groupes des complexes de module 1, et $(\mathbb{U}_n, \times)$ le groupe des racines $n^{\text{ième}}$ de l'unité.
- $(\mathfrak{S}(E), \circ)$ le groupe des permutations sur un ensemble E quelconque.
- $(\mathrm{GL}(E), \circ)$ le groupe linéaire de E.
- $(\mathrm{SL}(E), \circ)$, $(\mathrm{O}(E), \circ)$, $(\mathrm{SO}(E), \circ)$
- Les groupes des isométries d'une figure (groupes diédraux par exemple).

I.3 Sous-groupes

Proposition (Test du sous-groupe)

Soit $(G, \cdot)$ un groupe, et soit $H \subset G$. Alors H est un sous-groupe de G si et seulement si les deux conditions suivantes sont vérifiées :

i. $H \neq \emptyset$

ii. $\forall (x, y) \in H^2$, $xy^{-1} \in H$

Un exemple de référence : les sous-groupes de $(\mathbb{Z}, +)$

Proposition

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

Démonstration.

I.4 Intersections de sous-groupes

Comme toute les stuctures, la structure de groupe est stable par intersection et pas par réunion.

Proposition

Toute intersection de sous-groupes est un sous-groupe

I.5 Morphismes

Définition et vocabulaire

Définition

Soient $(G_1, \cdot)$ et $(G_2, \times)$ deux groupes et soit ϕ une application de G_1 dans G_2. On dit que ϕ est un morphisme (on parle parfois aussi d'homomorphisme) lorsque :

$$\forall\,(x,y) \in G_1^2,\ \phi(x \cdot y) = \phi(x) \times \phi(y)$$

Si $G_1 = G_2$, on dira que ϕ est un endomorphisme. Si ϕ est bijectif, on parlera d'isomorphisme. Un endomorphisme bijectif est appelé automorphisme.

Exemples de référence

Vérifions que les applications

- $\exp : \mathbb{C} \longrightarrow \mathbb{C}^*$
- $\det : \mathrm{GL}_n(\mathbb{K}) \longrightarrow \mathbb{K}^*$
- $\epsilon : \mathfrak{S}_n \longrightarrow \{-1, 1\}$

sont des morphismes de groupes (en précisant pour quelles lois).

Propriétés des morphismes de groupe

Proposition (Composition)

Soient $f : G_1 \longrightarrow G_2$ et $g : G_2 \longrightarrow G_3$ deux morphismes. Alors $g \circ f$ est un morphisme de G_1 dans G_3.

Proposition (Inverse)

Si $f : G_1 \longrightarrow G_2$ est un morphisme bijectif, alors $f^{-1} : G_2 \longrightarrow G_1$ est aussi un morphisme.

On dit que f est un **isomorphisme de groupe** et que les groupes $(G_1, \cdot)$ et $G_2, \times)$ sont **isomorphes.**

Proposition (Image du neutre et de l'inverse)

Si ϕ est un morphisme de G dans G', alors $\phi(e_G) = e_{G'}$. Aussi, si $x \in G$, $\phi(x^{-1}) = (\phi(x))^{-1}$.

Proposition (Image directes et réciproques de sous-groupes)

Soit $\phi : G \longrightarrow G'$ un morphisme. Alors :
- Si H est un sous-groupe de G, alors $\phi(H)$ est un sous-groupe de G'.
- Si K est un sous-groupe de G', alors $\phi^{-1}(K)$ est un sous-groupe de G.
- En particulier, $\operatorname{Im}\phi$ et $\ker\phi$ sont des sous-groupe respectifs de G' et de G.
- le morphisme ϕ est injectif si et seulement si $\ker\phi = \{e_G\}$.

Exemples

Quels sont les noyaux des trois morphismes de référence ?

I.6 Partie génératrice d'un groupe

Une union de groupes n'est pas un groupe. On cherche une notion qui remplace la réunion.

Définition

Soit G un groupe. Soit $A \subset G$ un ensemble quelconque. On appelle sous-groupe engendré par A, noté $\langle A\rangle$, l'ensemble :

$$\langle A\rangle = \bigcap_{\substack{H \text{ sous-groupe} \\ H \supset A}} H$$

On en déduit :
- G est un sous-groupe de G qui contient A donc $\langle A\rangle \neq \emptyset$
- $\langle A\rangle$ est bien un sous-groupe de G puisque l'intersection de sous-groupes est un sous-groupe.
- C'est le plus petit des sous-groupes contenant A (au sens de l'inclusion).

Définition d'une famille (ou partie) génératrice

Définition

Une partie A de G est dite génératrice si $G = \langle A\rangle$.

Ce notion ressemble un peu à la notion de partie génératrice des espaces vectoriels, mais elle est sensiblement plus compliquée.

Exemples.

- $\{1\}$ est une partie génératrice de $\mathbb{Z}$.
- l'ensemble des transpositions est une partie génératrice de groupe des permutations.
- : $\{3, 7\}$ est une partie génératrice de $\mathbb{Z}$.
- : Quel est le sous groupe de $GL_2(\mathbb{R})$ engendré par les matrices orthogonales S_θ ?

d'une manière générale, dans un groupe dont la loi est notée multiplicativement, si on a une famille A d'éléments, alors le groupe engendré par A est l'ensemble de tous les éléments obtenus en faisant des produits et des inverses

à partir des éléments de A :

$$\langle A\rangle = \{x_1 \times \cdots \times x_p,\ x_i \in A \text{ ou } x_i^{-1} \in A\}$$

Démontrer ce fait constitue un bon exercice de cours.

Un dernier exemple : famille génératrice du groupe SL_n

Soit $M \in \mathcal{M}_n(\mathbb{C})$ une matrice de déterminant 1. Alors d'après le pivot de Gauss, il existe $T_1, ..., T_r, ...T_p$ des matrices de transvections telles que :

$$M = T_1 \times \cdots \times T_r \times \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \det M \end{pmatrix} \times T_{r+1} \times \cdots \times T_p$$

En théorie des groupes ce résultat s'interprète de la façon suivante : le goupr $\mathrm{SL}_n(\mathbb{R})$ (matrices de déterminant 1) est engendré par les matrices de transvections.

II Groupes monogènes et cycliques

II.1 Définition

Définition

Un groupe G est dit monogène s'il possède au moins une famille génératrice de cardinal 1. Si $\{x\}$ engendre G, on dit que x est un générateur de G.

Un groupe est dit **cyclique** si il est **monogène** et **fini.**

II.2 Deux exemples fondamentaux

Proposition

$\mathbb{Z}$ est monogène.
De plus $\mathbb{Z}$ il n'y a que deux générateurs : 1 et -1.

Proposition

Le groupe $\mathbb{U}_n$ des racines de l'unité est cyclique.

Nous allons maintenant introduire un nouveau groupe qui joue un rôle essentiel en arithmétique.

II.3 le groupe $\mathbb{Z}/n\mathbb{Z}$

Rappel sur les congruences.

Définition

On pose, pour $(x, y) \in \mathbb{Z}^2$, $xRy \iff x \equiv y[n]$. Alors R est une relation d'équivalence sur $\mathbb{Z}$ et possède n classes d'équivalences notés $\overline{0}, ..., \overline{n-1}$.

On note $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, ..., \overline{n-1}\}$ l'ensemble des classes d'équivalence.

Définition

L'application $j : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ qui à un entier x dans $\mathbb{Z}$ associe $\overline{x}$ sa classe d'équivalence modulo n est appelée **surjection canonique**.

Description sur les exemples $n = 2$ et $n = 5$.

Proposition (Structure de groupe additif)

- : l'addition est compatible avec la relation d'équivalence R, c'est à dire que :

$$\left.\begin{array}{l} x \equiv x'\,[n] \\ y \equiv y'\,[n] \end{array}\right\} \Longrightarrow x + y \equiv x' + y'\,[n]$$

- La définition $\overline{x} + \overline{y} = \overline{x+y}$ est non ambigüe et définit une loi de composition sur $\mathbb{Z}/n\mathbb{Z}$.

- Muni de cette loi $\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique.

Démonstration :

Pourquoi le groupe $\mathbb{Z}/n\mathbb{Z}$ est il si important ? il y a deux raisons
La première est qu'il va permettre de faire de l'arithémtique modulaire (travailler avec des congruences de façon formelle) : nous verrons ceci plus tard.
La seconde est qu'il constitue en quelque sorte le prototype du groupe cyclique. En effet, on a l'important théorème suivant :

II.4 Théorème de classification des groupes monogènes

Théorème de classification

i. $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique.

ii. Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.

iii. Tout groupe cyclique de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration.

II.5 Exemples d'utilisation

Diverses écritures des de la Liste des éléments d'un groupe cyclique.

Démontrons que tout groupe cyclique est abélien (la réciproque est fausse).

Démontrons que tout groupe cyclique de cardinal n possède un sous groupe cyclique de cardinal d si d divise n.

III Eléments d'ordre fini dans un groupe

III.1 Éléments d'ordre fini dans un groupe.

Un morphisme de groupes associé à $a \in G$

Soit G un groupe, et soit $a \in G$. On pose :

$$\phi_a : \begin{vmatrix} \mathbb{Z} & \longrightarrow G \\ n & \longmapsto a^n \end{vmatrix}$$

Alors ϕ_a est un morphisme et $\operatorname{Im} \phi_a$ est le sous-groupe monogène engendré par a.

On a deux situations possible et seulement deux :

Le morphisme ϕ_a est injectif :
Dans ce cas, le groupe monogène engendré par a est infini. Les éléments $(a^n)_{n\in\mathbb{N}}$ sont tous distincts. On dit que a **n'est pas d'ordre fini.**

La deuxième situation nécessite une étude plus détaillée :

Élément d'ordre fini

Définition

On dit que a est d'ordre fini s'il vérifie l'une des propriétés équivalentes suivantes suivantes :

— $\exists\, n_0 \neq 0,\ a^{n_0} = 1_G$.
— $\exists n \neq m, : a^n = a^m$ (autrement dit ϕ_a n'est pas injective).

Démonstration

Définition

Si a est d'ordre fini, on appelle ordre de a le plus petit entier n_0 strictement positif tel que $a^{n_0} = 1_G$. Il est souvent noté $\omega(a)$ ou $o(a)$.

Exemples
Soit x un élément d'un groupe tel que $x^7 = x^{11}$. Justifier que x est d'ordre fini. Que peut on dire à priori de son ordre ?

Soit $M \in O_2(\mathbb{R})$. Etudier si M est d'ordre fini et déterminer l'ordre.

III.2 Propriétés de l'ordre

Proposition

Soit $a \in G$ un élément d'ordre fini. Alors $\omega(a)$ est le cardinal du sous-groupe (cyclique) engendré par a. On a donc $< a >= \{1, a, \ldots, a^{\omega(a)-1}\}$

Le neutre est d'ordre 1 et c'est le seul.
Si a est d'ordre fini, alors son inverse aussi et $o(a^{-1}) = o(a)$.
l'image par un morphisme d'un élément d'ordre fini est aussi d'ordre fini.

Démonstration :

Le résultat qui vient maintenant est important : pour l'illustrer reprenons l'exemple d'un élément x qui vérifie $x^7 = x^{11}$. Nous avons vu que $x^4 = e$ donc l'ordre est inférieur ou égal à 4. On peut en fait dire bien mieux.

Proposition

Si a est d'ordre fini $\omega(a)$ alors on a l'équivalence :

$$a^n = 1 \Leftrightarrow \omega(a)|n$$

Démonstration

Exemple. Soit x tel que $x^{11} = x^7 = 1$. Alors :

III.3 Caractérisation des groupes cycliques

bien qu'immédiat, ce théorème est important dans la pratique :

Proposition

Un groupe fini G est cyclique si et seulement si il existe un élément x dont l'ordre est égal à $|G|$

Exemple
Le groupe $\mathfrak{S}_3$ est il cyclique ?

III.4 Le théorème de Lagrange

Le résultat suivant, plus difficile, est très utile en théorie des groupes

Théorème

Si G est fini, tout élément a de G est d'ordre fini, et $\omega(a)$ divise le cardinal de G.
Si G est fini, pour tout $x \in G$, $x^{|G|} = 1$.

Démonstration
On la fait, conformément au programme, seulement dans le cas commutatif.

Ce théorème peut avoir de très puissantes applications. en voici quelques unes

Groupes de cardinal 7

Sous groupes finis de $(\mathbb{C}^*, \cdot)$

III.5 Propriétés complémentaires de l'ordre

A titre d'exercice on pourra démontrer les deux résultats suivants
- si x est d'ordre p et k divise p, alors x^k est d'ordre p/k.

- (très classique)Si x et y commutent et ont des ordres p, q premiers entre eux alors l'ordre de xy est d'ordre pq.

III.6 Complément : Détermination des générateurs

On commence par le cas du groupe cyclique de référence :

Proposition

On se place dans $(\mathbb{Z}/n\mathbb{Z}, +)$. Soit $k \in [\![0, n-1]\!]$.

$$\omega(\overline{k}) = \frac{n}{n \wedge k}$$

Démonstration.

Théorème

Les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les $\overline{k}$ lorsque k est un enier premier avec n.

Corollaire

Les générateurs de $\mathbb{U}_n$ sont les **racines primitives $n$ièmes de l'unité**, c'est à dire les $e^{(2ik\pi)/n}$ avec $\text{pgcd}(k, n) = 1$.

Illustrons cette situation par différents exemples.

III.7 Complément (HP) Sous groupes des sous-groupes cycliques

Théorème

— Tout sous-groupe d'un groupe cyclique est cyclique.
— Pour tout diviseur d de $n = |G|$, il existe un unique sous-groupe de G de cardinal d et celui-ci est cyclique.

IV Annexe 1 : rappels sur le groupe symétrique

Dans cette partie, on notera systématiquement n le cardinal d'un ensemble E. $\mathfrak{S}(E)$ désigne l'ensemble des permutations sur E. Notons que le cardinal de cet ensemble vaut $n!$.

Proposition

$\mathfrak{S}(E)$ est isomorphe à $\mathfrak{S}_n \overset{\text{def}}{=} \mathfrak{S}(\llbracket 1, n \rrbracket)$.

Démonstration. On considère $f : E \longrightarrow \llbracket 1, n \rrbracket$ bijective. Alors g est un isomorphisme de $\mathfrak{S}_n$ sur $\mathfrak{S}(E)$:

$$g : \begin{vmatrix} \mathfrak{S}_n & \longrightarrow \mathfrak{S}(E) \\ \sigma & \longmapsto f^{-1} \circ \sigma \circ f \end{vmatrix}$$

IV.1 Cycles

Définition

On nomme p-cycle et on note $(a_1, ..., a_p)$ la permutation $\sigma \in \mathfrak{S}_n$ suivante :

$$\sigma : \begin{vmatrix} \llbracket 1, n \rrbracket & \longrightarrow \llbracket 1, n \rrbracket \\ i & \longmapsto \begin{cases} \sigma(i) = i \text{ si } i \notin \{a_1, ..., a_p\} \\ \sigma(a_k) = a_{k+1} \text{ si } k < p \\ \sigma(a_p) = a_1 \end{cases} \end{vmatrix}$$

$\{a_1, ..., a_n\}$ est dit le <u>support</u> du p-cycle.

Proposition

- Un p-cycle est d'ordre p.
- Deux cycles à supports disjoints commutent.
- Tous les p-cycles sont conjugués.

Démonstration. On démontre le troisième point. Soit σ une permutation de $\mathfrak{S}_n$. Soit $j \in \llbracket 1, n \rrbracket$ tel qu'il existe $i \in \llbracket 1, p \rrbracket$ tel que $j = \sigma(a_i)$. $\sigma \circ (a_1, ..., a_p) \circ \sigma^{-1}(j) = \sigma(a_{i+1})$. Si $j \notin \{\sigma(a_1), ..., \sigma(a_p)\}$, $\sigma \circ (a_1, ..., a_p) \circ \sigma^{-1}(j) = j$. Ainsi, il nous suffit de prendre σ telle que pour tout $i \in \llbracket 1, n \rrbracket$, $\sigma(a_i) = b_i$.

IV.2 Décomposition en produits de cycles disjoints

Théorème

Soit $\sigma \in \mathfrak{S}_n$. Il existe une famille $\sigma_1, ..., \sigma_p$ de cycles à support disjoints telle que $\sigma = \sigma_1 \circ \cdots \circ \sigma_p$. Celle-ci est unique à l'ordre près des facteurs.

Démonstration. (abrégée)
On définit R une relation binaire sur $\llbracket 1, n \rrbracket$: $xRy \iff \exists\, k,\ \sigma^k(x) = y$. Il est facile de voir que R est une relation d'équivalence. On montre ensuite que sur chaque classe d'équivalence, σ est un cycle. Comme les classes d'équivalences sont disjointes et que les cycles à supports disjoints commutent, on a montré l'existence d'une telle famille. Pour l'unicité on suppose que $\sigma = \sigma_1 \circ \cdots \circ \sigma_i \circ \cdots \circ \sigma_p$ avec les σ_k des cycles à supports disjoints. Soit $x \in \llbracket 1, n \rrbracket$. Il existe un unique i tel que x appartienne au support de σ_i (on rajoute les cycles de taille 1). Alors le support de σ_i est égal à l'ensemble des $\sigma^k(x)$. On montre ainsi que la famille des σ_k est égale à la famille des cycles ayant pour support les classes d'équivalence de R.

Exercice : démontrer que deux permutation sont conjuguées si et seulement si elles ont des cycles de mêmes

longueur.

IV.3 Ordre d'une permutation

Proposition

Si $\sigma = \sigma_1 \circ \cdots \circ \sigma_k$ est la décomposition de σ en cycles disjoints de longueurs $p_1, ..., p_k$, alors l'ordre de σ est $\omega(\sigma) = \text{ppcm}(p_1, ..., p_k)$.

Démonstration. Posons $r = \text{ppcm}(p_1, ..., p_k)$. $\sigma^r = \sigma_1^r \circ \cdots \circ \sigma_k^r = id$ donc $\omega(\sigma)|r$. Soit x dans le support de σ_i. $\sigma^{\omega(\sigma)} = id$ donc $\sigma_i^{\omega(\sigma)}(x) = x$, d'où $p_i = \omega(\sigma_i)|\omega(\sigma)$. Ceci étant vrai pour tout $i \in [\![1, k]\!]$, $r|\omega(\sigma)$.

IV.4 Rappels sur la signature d'une permutation

Définition

Soit $\sigma \in \mathfrak{S}_n$. On dit que σ présente une inversion en (i, j) si $i < j$ et $\sigma(i) > \sigma(j)$.

Définition

On définit $\epsilon(\sigma)$ la signature de la permutation σ comme :

$$\epsilon(\sigma) = (-1)^{\text{nombre d'interversions de } \sigma} = \frac{\prod_{i<j} (\sigma(j) - \sigma(i))}{\prod_{i<j} (j - i)}$$

Proposition

- $\epsilon : (\mathfrak{S}_n, \circ) \longrightarrow (\mathbb{R}^*, \cdot)$ est un morphisme de groupe.
- C'est le seul morphisme non trivial entre ces deux groupe.
- $\ker \epsilon$ est un sous-groupe distingué appelé groupe alterné, noté $\mathcal{A}_n$.

$$|\mathcal{A}_n| = \frac{n!}{2}$$

Proposition

Les p-cycles ont tous la même signature que $(1, 2, ..., p) = (1, p)(1, p-1) \cdots (1, 2)$, c'est à dire $(-1)^{p-1}$.

Proposition

Soit $\sigma \in \mathfrak{S}_n$. On note k le nombre de cycles disjoints en comprenant les singletons. Alors $\epsilon(\sigma) = (-1)^{n-k}$.

Démonstration. Notons p_1,...,p_k les longueurs des cycles. $p_1 + \cdots + p_k = n$. Ainsi $\epsilon(\sigma) = \prod \epsilon(\sigma_i) = \prod (-1)^{p_i - 1} = (-1)^{n-k}$.

Exercice (génération de $\mathcal{A}_n$ par les trois cycles.
Démontrer que tous les $3-$cycles sont dans $\mathcal{A}_n$.

Démontrer Toute permutation de $\mathcal{A}_n$ est produit de trois-cycles.

Proposition

— $f_\sigma \in \mathrm{GL}(E)$
— $\sigma \in \mathfrak{S}_n \longmapsto f_\sigma \in \mathrm{GL}(E)$ est un morphisme de groupes injectif.

Définition

On note $M_\sigma = \mathrm{Mat}_b(f_\sigma)$. M_σ est la matrice de permutation associée à la permutation σ.
On note $\mathfrak{S} = \{M_\sigma,\ \sigma \in \mathfrak{S}_n\}$ l'ensemble des matrices de permutations.

Proposition

$\mathfrak{S}$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.
$M \in \mathfrak{S}$ si et seulement si M admet un unique coefficient non nul par ligne et par colonne, qui vaut 1.

V Annexe 2 : Classes modulo un sous-groupe : le théorème de Lagrange

Proposition Translation à gauche

Soit G un groupe, soit $a \in G$. On définit la translation à gauche τ_a ainsi :

$$\tau_a : \begin{vmatrix} G & \longrightarrow G \\ x & \longmapsto a \cdot x \end{vmatrix}$$

Proposition

Les translations à gauche sont bijectives, et $(\tau_a)^{-1} = \tau_{a^{-1}}$. (ce ne sont pas des morphismes !)

Définition

Soit H un sous-groupe de G, soit $a \in G$. On note :

$$aH = \{ah,\ h \in H\} = \tau_a(H)$$

Proposition

Pour tout $(a, b) \in G^2$, il existe une bijectin entre aH et bH .

Remarque. Le résultat précédent est immédiat, puisque les translations sont bijectives.

Définition

Soit H un sous-groupe de G. On définit sur G la relation $xR_Hy \iff x^{-1}y \in H$.

Proposition

R_H est une relation d'équivalence et les classes d'équivalences sont les classes à gauche modulo H.

Démonstration.
- R_H est réflexive.
- R_H est symétrique.

• Si xR_Hy et yR_Hz, alors $x^{-1}y \in H$ et $y^{-1}z \in H$, d'où par produit $x^{-1}z \in H$ et xR_Hz.
R_H est donc une relation d'équivalence
Montrons maintenant que pour tout $x \in H$, $\overline{x} = xH$.

$$\begin{aligned} y \in \overline{x} &\iff x^{-1}y \in H \\ &\iff \exists\, h \in H,\ y = xh \\ &\iff y \in xH \end{aligned}$$

Corollaire

Soient x et y deux éléments de G. Alors $y \in xH \iff yH = xH$.

Corollaire

Les classes à gauche modulo H forment une partition de G en sous-ensembles équipotents.

Remarque. En notation additive, si $a \in G$ et si H est un sous-groupe de G, on note $a + H$ les classes à gauche modulo H.

Exemple. Prenons $G = \mathbb{Z}$ et $H = n\mathbb{Z}$. Alors :

$$xR_Hy \iff y - x \in H \iff y - x \in n\mathbb{Z} \iff y \equiv x\ [n]$$

V.1 Classes à droite

Définition

Soit H un sous-groupe de G. On pose, pour $x \in G$, $Hx = \{hx,\ h \in H\}$.

En général, $xH \neq Hx$.

V.2 Sous-groupes distingués (HP)

Définition

Soit H un sous-groupe de G. On dit que H est distingué (ou normal) lorsque :

$$\forall\, x \in G,\ xH = Hx$$

Remarque. La condition équivaut aussi à :

$$\forall\, x \in G,\ \forall\, h \in H,\ \exists h' \in H,\ xh = h'x$$

ou encore à :

$$\forall\, x \in G,\ \forall\, h \in H,\ xhx^{-1} \in H$$

Exemple.
- Tous les sous-groupes de groupes abéliens sont distingués.
- G et $\{e_G\}$ sont distingués
- Si $f : G \longrightarrow G'$ est un morphisme de groupes, alors $\ker f$ est distingué.
- Le centre d'un groupe est toujours un sous-groupe distingué.

V.3 Le théorème de Lagrange

Théorème (Lagrange)

Soit G un groupe fini. Soit H un sous-groupe de G. Alors $|H|$ divise $|G|$.
En particulier, pour tout x dans G, l'ordre de x divise le cardinal de G.

Démonstration. G étant fini, les classes à gauche modulo H sont en nombre fini. On les notes a_1H,a_2H,...,a_pH. Comme G est l'union disjointe de ces classes, on sait que $|G| = |a_1H| + \cdots + |a_pH|$. Or, pour tout $i \in [\![1, p]\!]$, $|a_iH| = |H|$. Ainsi $|G| = p|H|$.

Pour la deuxième partie, il suffit de choisir pour H le groupe engendré par x.

VI Annexe 3 : Notions sur les actions de groupes

Définition

Soit G un groupe, soit E un ensemble. On appelle action (ou opération) du groupe G sur l'ensemble E une application "$\cdot$" ayant les propriétés suivantes :

$$\cdot : \begin{vmatrix} G \times E & \longrightarrow E \\ (g, x) & \longmapsto g \cdot x \end{vmatrix}$$

i. $\forall\, x \in E,\ e \cdot x = x$

ii. $\forall\, x \in E,\ \forall\, (g, g') \in G^2,\ (gg') \cdot x = g \cdot (g' \cdot x)$

Exemple. Soit G un groupe, on pose $E = G$. Alors la translation à gauche τ est une action de groupe :

$$\tau : \begin{vmatrix} G^2 & \longrightarrow G \\ (g, x) & \longmapsto g \cdot x \end{vmatrix}$$

Si l'on prend $G = (\mathbb{K}, \cdot)$ et E un $\mathbb{K}$-espace vectoriel, alors la loi externe sur cet espace vectoriel est une action de groupe :

$$\begin{vmatrix} (\mathbb{K}, \cdot) \times E & \longrightarrow E \\ (\lambda, x) & \longmapsto \lambda \cdot x \end{vmatrix}$$

Définition (Orbite sous l'action d'un groupe)

On se donne "$\cdot$" une action de G sur E, et on considère la relation binaire R sur E suivante :

$$xRy \iff \exists\, g \in G,\ g \cdot x = y$$

Alors R est une relation d'équivalence et on appelle les orbites sous l'action de G les classes d'équivalences de R. Si $x \in E$, on note :

$$\mathcal{O}_x = \{g \cdot x,\ g \in G\}$$

Proposition

• Si U est un ensemble qui rencontre exactement une fois chaque orbite :

$$E = \bigsqcup_{x \in U} \mathcal{O}_x$$

• Si $y \in \mathcal{O}_x$, pour tout $g \in G$, $g \cdot y \in \mathcal{O}_x$. • Si $(y, y') \in (\mathcal{O}_x)^2$, alors il existe $g \in G$ tel que $y' = g \cdot y$. • Lorsque E est fini :

$$|E| = \sum_{x \in U} |O_x|$$

Proposition

Si G est fini, chaque orbite est finie et $|\mathcal{O}_x|$ divise $|G|$.
Plus précisément, si on pose $G_x = \{g \in G,\ g \cdot x = x\}$:

$$|\mathcal{O}_x| = \frac{|G|}{|G_x|}$$

Démonstration. Soit $x \in E$. On remarque que G_x est un groupe (appelé stabilisateur de x). Soit $g \in G$. $gG_x = \{gg_1, g_1 \in G_x\}$.

$$\begin{aligned} g_1 \in G_x &\iff g_1 x = x \\ &\iff g g_1 x = gx \end{aligned}$$

Ainsi, $gG_x = \{h \in G,\ hx = gx\}$. Alors :

$$G = \bigsqcup_{y \in \mathcal{O}_x} \{g \mid g \cdot x = y\}$$

est une union de classes à gauche modulo G_x. On a donc :

$$|G| = \sum_{y \in \mathcal{O}_x} |G_x| = |\mathcal{O}_x| \times |G_x|$$

Exercice : faire le lien entre ce résultat et le premier théorème d'isomorphisme.

On en déduit directement la formule suivante très utile pour les calculs de cardinaux dans les groupes :

Proposition (Équation aux classes)

Si E et G sont finis :

$$|E| = \sum_{x \in U} \frac{|G|}{|G_x|}$$

Exemple. On peut montrer (exercice) en utilisant l'équation aux classes et l'action de G sur lui meme par conjugaison que le centre d'un p-groupe est non trivial. Cependant on peut aussi montrer (autre exercice, facile) que le centre d'un groupe ne peut pas être d'indice un nombre premier (considérer le sous groupe engendré par un élément x et le sous groupe $Z(G)$.) En conséquence, si p est premier, tout groupe de cardinal p^2 est abélien.

Un autre exercice (plus difficile) est de montrer que si H est un sous-groupe strict de G fini, alors :

$$\bigcup_{x \in G} xHx^{-1} \neq G$$