Groupes et sous groupes

1. Définitions et exemples

Un groupe est un ensemble G muni d'une loi de composition (ou loi de groupe ou produit)

c'est à dire une application $G\times G \to G$; $(a,b)\mapsto a\cdot b$

[dans la notation produit] qui vérifie les axiomes suivants

(i) $\forall a,b,c \in G ; (a\cdot b)\cdot c = a\cdot(b\cdot c)$ associativité

(ii) il existe $e\in G$ tq $a\cdot e = e\cdot a$ existence de l'élément neutre

(iii) $\forall x\in G, \exists y\in G$ tq $xy=yx=e$ existence de l'inverse

Remarques a) l'élément neutre est unique : si e et e' vérifie (ii)

alors $e=ee'=e$

b) l'inverse de x est unique et noté x^{-1} :

si $xy=e=yx$, $xy'=e=y'x$; alors $y'(xy) = y'e = y'$

$$\begin{aligned} &y'(xy) = y'\cdot e = y' \\ &\;\;\,\| \\ &(y'x)\cdot y = e\cdot y = y \end{aligned}$$

c) $(x^{-1})^{-1}=x$; par unicité !

d) $(ab)^{-1}= b^{-1}a^{-1}$: en effet

$(b^{-1}a^{-1})\cdot(ab) = b^{-1}(a\cdot a^{-1})\cdot b = b^{-1}\cdot e\cdot b = b^{-1}b = e$; on conclut par unicité

Quelque cas particuliers

(i) si $\forall x,y\in G$ $x\cdot y = y\cdot x$ alors G est commutatif

Par exemple $(\mathbb{Z},+)$, $(\mathbb{R},+)$, $(\mathbb{Z}/p\mathbb{Z},+)$ sont commutatifs,

$(\mathbb{K},+)$, $(\mathbb{K}^*,\cdot)$ si $\mathbb{K}$ est un corps (et $\mathbb{K}^* := \mathbb{K}\setminus\{0\}$)

(ii) si G a un nombre fini d'éléments alors G est fini

L'intuition et des exemples

L'idée de groupe est d'abstraire la notion de "transformation d'un ensemble ». Comme nous allons le voir sur de nombreux exemples

(i) FONDAMENTAL Soit E un ensemble, l'ensemble $Bij(E)$ des bijections de E dans E est un groupe pour la loi de composition.

(ii) Si $E = \{1, \dots, n\}$ on note $\mathfrak{S}_n := Bij(E)$, le groupe symétrique. Le groupe $\mathfrak{S}_n$ est fini et $\# \mathfrak{S}_n = n!$

(iii) Soit E un espace vectoriel, le groupe

$$GL(E) := End(E) \cap Bij(E)$$
$$= \{ f \text{ linéaire et inversible} \}$$

est le groupe général linéaire.

(iv) Si $\mathbb{K}$ est un corps, $GL_n(\mathbb{K}) = \{$matrice $(n \times n)$, à coefficients de $\mathbb{K}$ de déterminant non nul$\}$

(v) un espace vectoriel E est un groupe commutatif

2. Morphismes et isomorphismes

Une application f de $G \to H$, où G et H sont des groupes, est un morphisme (de groupe) si $\forall x, y \in G$: $f(x \cdot y) = f(x) \cdot f(y)$

Exemples (i) si $f \in End(E)$, alors f est un morphisme (du groupe E)

(ii) $\det : GL(E) \to \mathbb{K}^*$ est un morphisme de groupe

(iii) si $g \in G$: $f \mapsto g f g^{-1}$ est un morphisme dit de conjugaison par g.

(iv) il existe un unique morphisme appelé signature $\varepsilon : \sigma \mapsto \varepsilon(\sigma)$, $\mathfrak{S}_n \to \{-1, 1\}$ tel que $\varepsilon(\tau) = -1$ pour toute transposition τ.

3. Sous groupes

Soit G un groupe, $H \subset G$ est un sous groupe si

(i) $\forall f, g \in H$; $fg^{-1} \in H$

rk : $e = ff^{-1} \in H$; $f^{-1} = e.f \in H$, $fg \in H$

de telle sorte que (i) $\Leftrightarrow$ (i)' $fg \in H$ + (ii)' $f^{-1} \in H$, $\forall f, g \in H$

propriétés

(i) la restriction du produit a un sous-groupe lui donne une structure de groupe

(ii) Si $H, F \subset G$ sont des sous groupes alors $H \cap F$ est un sous-groupe

Exemples (i) $GL(E) \subset Bij(E)$

(ii) $SL(E) := \{ f \in GL(E) \mid \det f = 1 \} \subset GL(E)$

est le groupe spécial linéaire

(iii) Si (E, q) est un espace vectoriel muni d'une forme quadratique non dégénérée q alors le groupe orthogonal de q

$$O_q(E) = \{ f \in GL(E) \mid q(f(u)) = q(u) \, ; \forall u \in E \}$$

est un sous-groupe de $GL(E)$

Soit S un ensemble inclus dans G, le sous groupe engendré par S dénoté $\langle S \rangle$ est l'intersection de tous les sous groupes contenant S

rk : (i) $\langle S \rangle$ est un sous-groupe

(ii) si S est fini : $S = \{ s_1, \dots, s_n \}$

$$\langle S \rangle = \{ \underbrace{s_{i_1}^{n_{i_1}} \cdots s_{i_j}^{n_{i_j}}}_{\text{mots dans l'alphabet } S} , \; i_k \in \{1, \dots, n\} \; ; \; n_{i_j} \in \mathbb{Z} \}$$

Un groupe G est finiment engendré si il existe un ensemble fini S tel que $G = \langle S \rangle$

exemples (i) $\mathbb{Z}$, groupe fini, sont finiment engendré, (ii) $\mathbb{R}$ n'est pas finiment engendré car non dénombrable, (iii) $\mathbb{Q}$ n'est pas finiment engendré.

Théorème : Soit f un morphisme $G \to F$

(a) $f(G)$ est un sous groupe de F

(b) $\operatorname{Ker} f := f^{-1}(e)$ est un sous-groupe de G

◀ Exercice ▶

4. Un exemple important : le groupe libre

Théorème : Soit S un ensemble, il existe alors un groupe F_S et une injection i de $S \to F_S$ tel que pour tout groupe G, pour toute application $h : S \to G$; il existe un unique morphisme $H : F_S \to G$ tel que $h = H \circ i$

De plus (F_S, i) sont unique à isomorphisme près : si (F_S', i') vérifient les conditions du théorème, il existe alors un isomorphisme $\varphi : F_S \to F_{S'}$, tel que $i' = \varphi \circ i$

Graphiquement, on dit le diagramme

$$\begin{tikzcd} F_S \arrow[dr, "H"] & \\ S \arrow[u, "i"] \arrow[r, "h"'] & H \end{tikzcd}$$

commute

En general un diagrame

$$\begin{tikzcd} & E_2 \arrow[r, "f_2"] & E_3 \arrow[dr, "f_5"] & & \\ E_1 \arrow[ur, "f_1"] \arrow[dr, "f_3"'] & & & E_5 \arrow[r] & E_6 \\ & E_2 \arrow[uur, "f_3"] \arrow[urr, "f_4"'] & & & \end{tikzcd}$$

commute si dès qu'on a un cycle de flèches

Alors $f_3 \circ f_2 \circ f_1 = g_2 \circ g_1$

$$\begin{tikzcd} & \bullet \arrow[r, "f_2"] & \bullet \arrow[dr, "f_3"] & \\ E \arrow[ur, "f_1"] \arrow[dr, "g_1"'] & & & \bullet \\ & \bullet \arrow[urr, "g_2"'] & & \end{tikzcd}$$

◀ (i) unicité :

$$\begin{tikzcd} & F_S \arrow[d, "\varphi"] \\ S \arrow[ur, "i"] \arrow[r, "i'"'] & F_{S'} \end{tikzcd}$$

Il existe φ tq $i' = \varphi \circ i$

φ' tq $i = \varphi' \circ i'$

En particulier $i = (\varphi' \circ \varphi) \circ i$, alors par unicité du morphisme

dans le cas $\begin{tikzcd} & F_S \arrow[d] \\ S \arrow[ur, "i"] \arrow[r, "i"'] & F_S \end{tikzcd}$ On a $\varphi' \circ \varphi = Id$, de même $\varphi \circ \varphi' = Id$.

(ii) Existence.

Un mot dans l'alphabet S est une expression

$$w = s_1^{n_1} \cdots s_p^{n_p} \quad \text{tel que} \quad n_i \in \mathbb{Z}^* ; \quad s_j \in S$$

un mot est réduit si $s_i \neq s_{i+1}$, on considère le mot vide $e = \emptyset$

On a une projection $\{\text{mot}\} \to \{\text{mots réduits}\}$

On considère $J = \{ j$ tel que $s_j \neq s_{j+1} \}$, par convention $n \in J$

On remplace le mot $s_1^{n_1} \cdots s_p^{n_j} = W$

$$Q(W) = s_{j_1}^{m_1} \cdots s_{j_q}^{m_p} \quad \text{où } J = \{ j_1, \dots, j_q \}$$

$$m_k = \sum_{i = j_k + 1}^{j_k} n_k \; ; \quad \text{si } m_k = 0, \text{ on efface le terme } s_{j_1}^0$$

On itère ensuite la construction, et posant

$$w^{(n)} = \underbrace{Q \circ \cdots \circ Q}_{n}(w)$$

Au bout d'un temps fini on a $w^{(n+1)} = w^{(n)} = \mathcal{S}(w^{(n)})$

le mot $w^{(n)}$ est donc réduit et on pose $w^{(n)} = \pi(w)$.

$w^{(n)}$ peut être le mot vide.

Si w_1 et w_2 sont deux mots, leur concaténation est

$w_1 \# w_2$ = les deux mots écrits à la suite. On a

$$(w_1 \# w_2) \# w_3 = w_1 \# (w_2 \# w_3)$$

le groupe libre F_S est alors

$$F_S = \{\text{mots réduits}\}$$

$$w_1 \cdot w_2 = \pi(w_1 \# w_2)$$

L'élément neutre est $e = \emptyset$, l'inverse de

$$s_1^{n_1} \cdots\cdots s_p^{n_p} \text{ est } s_p^{-n_p} \cdots\cdots s_1^{-n_1}$$

On a une injection naturelle de $S \to F_S$, l'unique morphisme H de la définition est

$$H(s_1^{n_1} \cdots s_p^{n_p}) = h(s_1)^{n_1} \cdots h(s_p)^{n_p}$$

On note $F_n = F_{\{1,\dots,n\}}$

(i) en particulier $F_1 = \mathbb{Z}$