1. Groupes

1.1. Généralités

1.1.1. Premières définitions

Définition 1.1 (Groupes)

On appelle *groupe* un ensemble G muni d'une loi de composition interne notée $\cdot$ vérifiant les propriétés suivantes :

1. $\forall g, h, k \in G, (g \cdot h) \cdot k = g \cdot (h \cdot k)$ (associativité)
2. $\exists e \in G, \forall g \in G, e \cdot g = g \cdot e = g$ (existence d'un élément neutre, noté e)
3. $\forall g \in G, \exists h \in G, g \cdot h = h \cdot g = e$ (tout élément g admet un symétrique) [a]

Si la loi $\cdot$ est commutative, on dit que le groupe est *commutatif* (ou *abélien*). On appelle *ordre* du groupe le cardinal de G (qui peut être fini ou infini).

a. Lorsque la l.c.i. est notée multiplicativement, le neutre est noté 1 et le symétrique d'un élément g est appelé *inverse* de g, noté g^{-1}, et lorsque la l.c.i. est notée additivement, le neutre est noté 0 et le symétrique d'un élément g est appelé *opposé* de g et est noté $-g$.

Exemples. *1.* $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{Q}^*, \times), (\mathbb{R}^*, \times)$ *sont des groupes.*

2. Pour tout $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +)$ *et* $(\mathbb{Z}/n\mathbb{Z}^*, \times)$ *sont des groupes.*

3. $(\mathfrak{S}(X), \circ)$*, groupe des permutations d'un ensemble* X *.*

4. $(\mathcal{D}_n, \circ)$*, groupe diédral d'ordre* $2n$*, pour* $n \geqslant 3$*.*

5. $(GL(E), \circ)$*, groupe linéaire d'un espace vectoriel* E*.*

Définition et théorème 1.2 (Sous-groupes)

Soit G un groupe, une partie non-vide $H \subset G$ est appelée *sous-groupe* de G si elle est stable par la l.c.i. et par passage à l'inverse, autrement dit si

$$\forall h_1, h_2 \in H, h_1 \cdot h_2^{-1} \in H$$

Soit H un sous-groupe de G. Pour tout $g \in G$, les ensembles gH et Hg sont respectivement appelés *classe à gauche* et *classe à droite* de g selon H. L'ensemble des classes à gauche (resp. classes à droite) selon H se note G/H (resp. $H\backslash G$) et forme une partition de G.

DÉMONSTRATION $x \sim y \Leftrightarrow x^{-1}y \in H$ est une relation d'équivalence sur G, idem pour les classes à droite. □

Remarques. *1. Toute intersection de sous-groupes d'un groupe G est un sous-groupe de G.*

2. Pour toute partie A d'un groupe G, on note $< A >$ le sous-groupe de G engendré par A. C'est le plus petit sous-groupe de G contenant A.

3. Le sous-groupe de G engendré par les commutateurs de G, i.e. les éléments de la forme $(g_1g_2)(g_2g_1)^{-1}$, est appelé sous-groupe dérivé de G. C'est un sous-groupe caractéristique de G (cf. 5).

4. Le sous-groupe de G des éléments de G commutant avec tous les autres est appelé centre de G. C'est aussi un sous-groupe caractéristique de G.

Exemples. *1. Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.*

2. Les sous-groupes additifs de $\mathbb{R}$ sont soit denses soit de la forme $\alpha\mathbb{Z}$ avec $\alpha \in \mathbb{R}$.

Corollaire 1.3 (THÉORÈME DE LAGRANGE)

Soit G un groupe d'ordre fini et H un ss-groupe de G. Alors $|G| = |G/H| \cdot |H|$, en particulier l'ordre de tout sous-groupe de G divise l'ordre de G.

DÉMONSTRATION C'est un corollaire immédiat de la partition de G en classes selon H (à gauche ou à droite, au choix). Plus précisément, on a $|G/H| = |G|/|H| = |H\backslash G|$. □

Remarques. *1. En particulier pour tout élément g d'un groupe G fini, on peut définir l'ordre de g comme étant le cardinal de $< g >$: c'est aussi le plus petit entier n tel que $g^n = e$. Le théorème de Lagrange affirme que n est un diviseur de $|G|$.*

2. Si tous les éléments d'un groupe sont d'ordre fini, on appelle exposant le ppcm des ordres des éléments du groupe. Si le groupe est abélien fini, il existe un élément d'ordre l'exposant (cf. [29] p.26).

3. $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ et $\mathbb{Q}/\mathbb{Z}$ sont des groupes infinis dont tous les éléments sont d'ordre fini.

Comme corollaire immédiat, mentionnons le petit théorème de Fermat :

Application 1.4 (PETIT THÉORÈME DE FERMAT)

Soit p un entier premier et $x \in \mathbb{Z}$. Alors p divise $x^p - x$.

DÉMONSTRATION On se place dans le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$. Soit $x \in \mathbb{Z}/p\mathbb{Z}^*$ alors son ordre divise $|\mathbb{Z}/p\mathbb{Z}^*| = p - 1$ ce qui s'écrit $x^{p-1} = 1$ et par conséquent $x^p = x$. La dernière égalité est encore vraie si $x = 0$ dans $\mathbb{Z}/p\mathbb{Z}$. □

1.1.2. Sous-groupes distingués, groupes quotients, morphismes

Proposition 1.5 (GROUPE QUOTIENT)

Soit G un groupe et H un sous-groupe de G. La relation d'équivalence $x \sim y \Leftrightarrow x^{-1}y \in H$ est compatible à gauche avec la l.c.i. de G, i.e. :

$$\forall a, x, x' \in G \text{ t.q. } x \sim x', \text{ on a } ax \sim ax'$$

Idem pour la relation d'équivalence définissant les classes à droite : $x \sim y \Leftrightarrow xy^{-1} \in H$ qui est compatible à droite avec la l.c.i.

Lorsque H est *distingué* [a] dans G, i.e.

$$\forall g \in G, h \in H, ghg^{-1} \in H$$

ces deux relations d'équivalence définissent les même classes d'équivalence, i.e. les classes à gauche et à droite sont confondues. Cette relation d'équivalence est alors compatible à gauche et à droite avec la l.c.i., ce qui permet de munir l'ensemble quotient $G/H = H\backslash G$ d'une structure de groupe. [b]

a. On note alors $H \lhd G$.
b. Le cardinal de G/H est appelé *indice* de H dans G.

Exemples. *1.* $\mathfrak{A}_n \lhd \mathfrak{S}_n$, $SL_n(k) \lhd GL_n(k)$, $SO_n(\mathbb{R}) \lhd O_n(\mathbb{R})$, $\langle r \rangle \lhd \mathcal{D}_n$

2. Tout sous-groupe d'un groupe abélien est distingué. Contre-exemple : tout sous-groupe de $\mathbb{H}_8$ est distingué mais $\mathbb{H}_8$ n'est pas abélien (cf. [25] p.4).

3. $\mathbb{Z}/n\mathbb{Z}$ et $L^p = \mathcal{L}^p/\{$fonctions de $\mathcal{L}^p$ nulles p.p.$\}$ sont des groupes quotients.

Définition 1.6 (MORPHISMES DE GROUPES)

Soit $(G, \cdot)$ et $(G', *)$ deux groupes, on appelle *morphisme* de groupes de G dans G' toute application $\varphi : G \longrightarrow G'$ telle que

$$\forall g, h \in G, \varphi(g \cdot h) = \varphi(g) * \varphi(h) \text{ [a]}$$

Le *noyau* de φ défini par $\mathrm{Ker}(\phi) = \{g \in G; \varphi(g) = e'\}$ est un sous-groupe distingué de G.
L'*image* de φ définie par $\mathrm{Im}(\varphi) = \{\varphi(g); g \in G\}$ est un sous-groupe de G'. [b] [c]

a. Une telle application vérifie automatiquement $\varphi(e) = e'$ et $\forall g \in G, \varphi(g^{-1}) = \varphi(g)^{-1}$.
b. Si φ est bijectif, on dit que c'est un isomorphisme de groupes, si de plus $G = G'$ on dit que φ est un *automorphisme* de G.
c. Plus généralement, l'image et l'image réciproque de sous-groupes par un morphisme de groupes sont des sous-groupes, l'image réciproque d'un sous-groupe distingué est un sous-groupe distingué, l'image d'un sous-groupe distingué est un sous-groupe distingué de l'image.

Remarques. *1. Une partie $H \subset G$ est un sous-groupe distingué de G s-si H est noyau d'un morphisme de groupes de G dans G'.*

2. pour $n \in \mathbb{N}^*$, le groupe $U_n(\mathbb{C}) = \{e^{2ik\pi/n}; 0 \leqslant k < n\}$ des racines n-ièmes de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ via l'application $k \in \mathbb{Z}/n\mathbb{Z} \mapsto e^{2ik\pi/n} \in U_n(\mathbb{C})$.

3. Les morphismes de $(\mathbb{R}, +)$ dans $(\mathbb{R}, +)$ sont les $x \mapsto \lambda x$ avec $\lambda \in \mathbb{R}$.

Proposition 1.7 (Théorème de correspondance)

Soit G un groupe et $H \triangleleft G$ alors la projection canonique $\pi : G \to G/H$ induit une bijection entre les sous-groupes de G/H et les sous-groupes de G contenant H.

Démonstration Soit $\overline{K}$ un sous-groupe de G/H alors $K = \pi^{-1}(\overline{K})$ est un sous-groupe de G contenant H et $\overline{K} = \pi(K) = K/H$ d'où l'existence. Si K' sous-groupe de G contenant H vérifie $\pi(K') = \pi(K)$ alors pour tout $k' \in K'$ il existe $k \in K$ tel que $\pi(k') = \pi(k)$ donc $k' \in kH$ et comme $H \subset K$, $k' \in K$ donc $K' \subset K$ et par symétrie $K \subset K'$ donc $K = K'$ d'où l'unicité. □

Application 1.8 (Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$)

Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/(n/d)\mathbb{Z}$ où $d|n$.

1.1.3. Théorèmes d'isomorphisme

Théorème 1.9 (Premier théorème d'isomorphisme)

Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes. Alors $G/\mathrm{Ker}(\varphi) \simeq \mathrm{Im}(\varphi)$

Démonstration $H = \mathrm{Ker}(\varphi)$ est distingué dans G, donc $G/\mathrm{Ker}(\varphi)$ est bien un groupe. On note $\hat{\varphi}(xH) := \varphi(x)$ pour tout $x \in G$, cette définition ne dépend pas du représentant choisi, et on vérifie facilement que $\hat{\varphi}$ est un morphisme de groupes injectif et surjectif sur $\mathrm{Im}(\varphi)$. □

Théorème 1.10 (Deuxième théorème d'isomorphisme)

Soit K et H deux sous-groupes d'un groupe G tels que $K \subset N_G(H)$ [a]. Alors $KH = HK$ est un sous-groupe de G, $H \lhd KH$, $K \cap H \lhd K$ et

$$KH/H \simeq K/(K \cap H)$$

a. En particulier si $H \lhd G$.

Démonstration La vérification que $HK = KH$ est un sous-groupe de G si le normalisateur de H contient K est aisée, tout comme la vérification $H \lhd KH$. On considère le morphisme $f : K \to HK/H$ défini par $f(k) := kH$ (composée de l'injection $j : K \to HK$ et de la surjection canonique $\sigma : HK \to HK/H$). f est un morphisme surjectif, de noyau $H \cap K$, et le premier théorème d'isomorphisme permet de conclure. □

Théorème 1.11 (Troisième théorème d'isomorphisme)

Soit $K \subset H \subset G$ trois groupes. On suppose $H \lhd G$ et $K \lhd G$. Alors

$$(G/K)/(H/K) \simeq G/H$$

Démonstration Le morphisme $f : G/K \to G/H$ défini par $f(xK) := xH$ pour tout $x \in G$ est bien défini, est surjectif et de noyau H/K, le premier théorème d'isomorphisme permet alors de conclure. □

1.2. Opération d'un groupe sur un ensemble

1.2.1. Généralités

Définition 1.12 (Opération d'un groupe sur un ensemble)

On dit qu'un groupe G opère sur un ensemble X s'il existe une application :

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \mapsto & g \cdot x \end{array}$$

satisfaisant les propriétés suivantes : [a]

1. $\forall g, g' \in G, \forall x \in X,\ g \cdot (g' \cdot x) = (gg') \cdot x$
2. $\forall x \in X,\ e \cdot x = x$

a. Cela revient à se donner un morphisme de G dans $\mathfrak{S}(X)$ (le groupe des permutations de X).

Définition 1.13

Soit G un groupe opérant sur un ensemble X.

1. Pour tout $x \in X$, on appelle *orbite* de x l'ensemble :
$$\mathcal{O}_G(x) = \{g \cdot x; g \in G\}$$
2. Les orbites forment une partition de X [a]. Lorsqu'il n'y a qu'une seule orbite, on dit que G opère *transitivement* sur X. Les éléments dont l'orbite est réduite à un point sont appelés *points fixes* de X sous l'action de G.
3. Lorsque l'action de G sur X est injective (i.e. le morphisme $G \to \mathfrak{S}(X)$ est injectif), on dit que G opère *fidèlement* sur X.
4. Pour tout $x \in X$, on appelle *stabilisateur* de x l'ensemble :
$$G_x = \{g \in G; g \cdot x = x\}.$$
C'est un sous-groupe de G. Lorsque tous les stabilisateurs sont triviaux, on dit que G opère *librement* sur X. Une action libre est fidèle.

a. La relation d'équivalence sous-jacente étant définie par $x \sim y \Leftrightarrow \exists g \in G$ t.q. $y = g \cdot x$

Remarques. *1. Tout sous-groupe H d'un groupe G donné agit sur G par translation à gauche :*
$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \mapsto & hg \end{array}$$
et aussi par translation à droite :
$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \mapsto & gh^{-1} \end{array}$$

2. Tout groupe G agit par conjugaison sur chacun de ses sous-groupes distingués ($H \triangleleft G$) :
$$\begin{array}{ccc} G \times H & \longrightarrow & H \\ (g, h) & \mapsto & ghg^{-1} \end{array}$$
Lorsque $H = G$:

a) cette opération est appelée automorphisme intérieur.

b) Le stabilisateur d'un élément $g \in G$ par conjugaison est appelé centralisateur de g.

c) L'ensemble des points fixes de G est appelé centre de G, c'est un sous-groupe caractéristique de G (cf. 5).

3. Tout groupe G agit sur l'ensemble de ses sous-groupes par conjugaison :
$$\begin{array}{ccc} G \times \mathcal{H}(G) & \longrightarrow & \mathcal{H}(G) \\ (g, H) & \mapsto & gHg^{-1} \end{array}$$
Le stabilisateur d'un sous-groupe H par conjugaison est appelé normalisateur de H.

4. *Soit H un sous-groupe (pas nécessairement distingué) d'un groupe G , alors G agit sur G/H par translation à gauche :*

$$\begin{array}{ccc} G \times G/H & \longrightarrow & G/H \\ (g, xH) & \mapsto & (gx)H \end{array}$$

et aussi par translation à droite :

$$\begin{array}{ccc} G \times H\backslash G & \longrightarrow & H\backslash G \\ (g, Hx) & \mapsto & H(xg^{-1}) \end{array}$$

5. *Soit G un groupe, son groupe des automorphismes $Aut(G)$ agit sur l'ensemble des sous-groupes de G :*

$$\begin{array}{ccc} Aut(G) \times \mathcal{H}(G) & \longrightarrow & \mathcal{H}(G) \\ (\sigma, H) & \mapsto & \sigma(H) \end{array}$$

Ses points fixes sont appelés sous-groupes caractéristiques de G.

6. *Soit G un groupe, son groupe des automorphismes intérieurs $Aut_{Int}(G)$ i.e. les $\varphi_g : h \mapsto ghg^{-1}$ agit aussi sur $\mathcal{H}(G)$. Ses points fixes sont les sous-groupes distingués de G.*

Exemples. 1. *Si X est un ensemble, $\mathfrak{S}(X)$ agit fidèlement et transitivement sur X.*

2. *L'action de $\mathcal{D}_3$ sur les sommets d'un triangle équilatéral est fidèle mais n'est pas libre.*

3. *$O_n(\mathbb{R})$ agit sur $\mathbb{R}^n$ par $(P, X) \mapsto PX$, ses orbites sont les sphères de centre 0.*

4. *Soit k un corps. $GL_n(k)$ agit sur $M_{n,p}(k)$ par $(P, M) \mapsto PM$, les orbites sont les matrices de même noyau.*

5. *$GL_p(k)$ agit sur $M_{n,p}(k)$ par $(P, M) \mapsto MP^{-1}$, les orbites sont les matrices de même image.*

6. *$GL_n(k)$ agit sur $M_n(k)$ par conjugaison $(P, M) \mapsto PMP^{-1}$. La classification des orbites est donnée par le théorème des invariants de similitude.*

7. *$GL_n(k) \times GL_p(k)$ agit sur $M_{n,p}(k)$ par $(P, M) \mapsto PMQ^{-1}$, les orbites sont les matrices de même rang.*

8. *$O_n(\mathbb{R})$ agit sur $M_n(\mathbb{R})$ (resp. $U_n(\mathbb{C})$ agit sur $M_n(\mathbb{C})$) par conjugaison. Cette action traduit le changement de base orthonormale (resp. unitaire). L'orbite d'une matrice de $S_n(\mathbb{R})$ contient une matrice diagonale.*

9. *$GL_n(k)$ agit sur $S_n(k)$ par congruence $(P, M) \mapsto PM^tP$. Deux matrices de $S_n(k)$ sont dans la même orbite s-si elles représentent la même forme quadratique. Si $k = \mathbb{R}$, l'invariant d'orbite est la signature.*

La proposition suivante énonce des propriétés élémentaires importantes concernant les orbites et stabilisateurs des éléments d'un ensemble sur lequel un groupe opère :

Proposition 1.14

Soit G un groupe opérant sur un ensemble X. Alors

1. Pour tout $x \in X$, l'application $G/G_x \longrightarrow \mathcal{O}_G(x) : \overline{g} \mapsto g \cdot x$ est bien définie et est bijective. [a]
2. Les stabilisateurs des éléments d'une même orbite sont conjugués : $\forall x \in X,\ G_{g\cdot x} = gG_xg^{-1}$

a. En particulier, si G est fini, les stabilisateurs des éléments d'une même orbite sont tous de même cardinal, ce qui est aussi une conséquence du deuxième point.

1.2.2. Action d'un groupe fini sur un ensemble fini

Dans le cas où G et X sont tous deux de cardinal fini, on a alors :

Corollaire 1.15 (Formule des classes et formule de Burnside)

Soit G un groupe fini opérant sur un ensemble fini X. On note $(X_i)_{1\leqslant i\leqslant r}$ l'ensemble des orbites. Alors

1. $|X| = \displaystyle\sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}$
   $(x_i)_{1\leqslant i\leqslant r}$ étant un système de représentants quelconques de $(X_i)_{1\leqslant i\leqslant r}$ [a]
2. Le nombre r d'orbites est donné par $r = \dfrac{1}{|G|}\displaystyle\sum_{g\in G} |X^g|$
   où $X^g = \{x \in X; g \cdot x = x\}$ [b]

a. Cette formule est appelée *équation aux classes.*
b. X^g est l'ensemble des éléments fixes de X sous l'action de $< g >$. C'est la formule de Burnside.

Démonstration Le premier point est une conséquence immédiate de la proposition ci-dessus. Pour le deuxième point, considérer l'ensemble $E = \{(g, x); g \in G, x \in X \text{ t.q. } gx = x\}$. Son cardinal $|E|$ est indifféremment égal $\displaystyle\sum_{g\in G} |X^g|$ ou à $\displaystyle\sum_{x\in X} |G_x|$.

Or $\displaystyle\sum_{x\in X} |G_x| = \sum_{i=1}^{r} \sum_{x\in X_i} |G_x| = \sum_{i=1}^{r} |G|$ ce qui permet de conclure. □