Groupes (notes de cours)
Préparation à l'agrégation interne
Année 2016-2017, Université Paris Diderot

Catherine Gille

1 Groupes, sous-groupes, morphismes

Définition 1.1 *Un groupe est un ensemble G non vide muni d'une loi de composition interne associative, possédant un élément neutre, et tel que tout élément de G admet un inverse (= un symétrique). Si la loi est commutative, on dit que le groupe est commutatif (ou abélien).*

Remarque : unicité de l'élément neutre, de l'inverse

Notations multiplicative et additive (celle-ci étant réservée aux groupes commutatifs).

Définition du produit cartésien de deux groupes.

Exemples :
1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de $+$.
2. $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ munis de $\times$.
3. $(\mathbb{Z}/n\mathbb{Z}, +)$.
4. $(\mathcal{M}_n(\mathbb{K}), +)$, $(GL_n(\mathbb{K}), \times)$.
5. $(\mathcal{S}(E), \circ)$ groupe des bijections d'un ensemble E. Groupe symétrique $(\mathcal{S}_n, \circ)$.

Proposition 1.2 *Soit $(G, \cdot)$ un groupe et H une partie de G. Alors les propriétés suivantes sont équivalentes :*

a. H est stable pour la loi $\cdot$ et $(H, \cdot)$ est un groupe,

b. H est non vide, stable pour la loi $\cdot$ et stable par passage à l'inverse,

c. H est non vide et vérifie : $\forall (x, y) \in H^2, x \cdot y^{-1} \in H$.

Si a, b ou c est vérifié, on dit que H est un *sous-groupe* de G.

Proposition 1.3 *Une intersection de sous-groupes est un sous-groupe.*

Exemples :
1. $]0, +\infty[$ est un sous-groupe de $(\mathbb{R}^*, \times)$.
2. $\mathbb{U}_n = \{z \in \mathbb{C} | z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$, et même de $(S^1, \times)$.

3. Les sous-groupes de $(\mathbb{Z},+)$ sont les $m\mathbb{Z}$, $m \in \mathbb{N}$.
4. Les sous-groupes de $(\mathbb{R},+)$ sont soit de la forme $\alpha\mathbb{Z}$ ($\alpha \in \mathbb{R}$), soit denses dans $\mathbb{R}$ (cf exercice ci-dessous).
5. Centre d'un groupe : $Z(G) = \{a \in G | \forall x \in G, ax = xa\}$

Exercice 1.4 (Sous-groupes de $\mathbb{R}$) *1. Soit G un sous groupe de $(\mathbb{R},+)$, non réduit à $\{0\}$.*

(a) Montrer que si $\inf(G \cap]0,+\infty[) > 0$, alors G est de la forme $\alpha\mathbb{Z}$, avec $\alpha > 0$. (G est alors discret)

(b) Montrer que si $\inf(G \cap]0,+\infty[) = 0$ alors G est dense dans $\mathbb{R}$.

2. Soit $\delta \in]0,+\infty[$. Montrer que $G = \{a + b\delta,\ (a,b) \in \mathbb{Z}^2\}$ est un sous-groupe additif de $\mathbb{R}$. Montrer que G est discret si et seulement si $\delta \in \mathbb{Q}$.

Exercice 1.5 *Montrer que le centre de $GL_n(\mathbb{K})$ est l'ensemble des matrices scalaires non nulles.*

Sous-groupe engendré par une partie

Soit $(G,\cdot)$ un groupe et soit A une partie non vide de G. on appelle *sous-groupe engendré par A* l'intersection de tous les sous-groupes de G qui contiennent A. C'est aussi le plus petit sous-groupe de G qui contient A. On le note $gr(A)$ ou $< A >$.

Proposition 1.6 *Soit $(G,\cdot)$ un groupe, A une partie non vide de G. Alors $gr(A)$ est l'ensemble des produits d'éléments de A et de leurs inverses.*

Exemples :
1. $n\mathbb{Z} = gr(\{n\})$ dans $(\mathbb{Z},+)$.
2. $\mathbb{U}_n = gr(\{e^{\frac{2i\pi}{n}}\})$ dans $(\mathbb{C}^*,\times)$.
3. $GL_n(\mathbb{K})$ est engendré par les matrices d'opérations élémentaires.

Morphismes de groupes (=homomorphismes)

Définition 1.7 *Soit $(G,*)$ et $(G',*')$ deux groupes. On dit qu'une application $f : G \to G'$ est un morphisme de groupes si : $\forall x,y \in G, f(x*y) = f(x) *' f(y)$.*

Remarque : on a alors $f(1_G) = 1'_G$ et $f(x^{-1}) = f(x)^{-1}$ pour tout $x \in G$.

Si f est un morphisme bijectif, on dit que c'est un *isomorphisme*, et on dit alors que G et G' sont *isomorphes*.

En utilisant que la composée de deux morphismes est encore un morphisme et que l'inverse d'un isomorphisme est un (iso-)morphisme, on définit le groupe des *automorphismes* du groupe G, que l'on note $(Aut(G),\circ)$.

Proposition 1.8 *L'image (respectivement l'image réciproque) d'un sous-groupe par un morphisme est un sous-groupe.*

En particulier, si $f : G \to G'$ est un morphisme de groupes, alors $Imf = f(G)$ est un sous-groupe de G' et $Kerf = \{x \in G | f(x) = 1_{G'}\}$ est un sous-groupe de G.

Proposition 1.9 *Soit $f : G \to G'$ un morphisme de groupes. Alors f est injective si et seulement si $Ker f = \{1_G\}$.*

Soit $f : G \to G'$ un morphisme de groupes. On remarque que si $x \in Ker f$ et $a \in G$, alors $axa^{-1} \in Ker f$. Ainsi $Ker f$ est stable par conjugaison.

Définition 1.10 *Soit G un groupe, H un sous-groupe de G. On dit que H est distingué dans G si : $\forall x \in G, \forall h \in H, xhx^{-1} \in H$.*

Remarque : dans un groupe commutatif, tout sous-groupe est distingué.

On vient de voir que le noyau d'un morphisme de groupes est distingué. Plus généralement on a :

Proposition 1.11 *L'image réciproque par un morphisme de groupes d'un sous-groupe distingué est un sous-groupe distingué.*

Exemples de morphisme :
0. Soit G un groupe et H un sous-groupe de G. Alors l'inclusion de H dans G est un morphisme de groupes injectif.
1. $\exp : (\mathbb{R}, +) \to (]0, +\infty[, \times)$ est un isomorphisme d'inverse ln.
2. $\det : (GL_n(\mathbb{R}), \times) \to (\mathbb{R}^*, \times)$ est un morphisme de groupes surjectif.
$SL_n(\mathbb{R}) = Ker \det$ est un sous-groupe distingué de $GL_n(\mathbb{R})$. L'ensemble des matrices $n \times n$ inversibles à déterminant positif est un sous-groupe distingué de $GL_n(\mathbb{R})$ (c'est $\det^{-1}(]0, +\infty[)$).
3. Signature des permutations : $\varepsilon : (\mathcal{S}_n, \circ) \to (\{-1, +1\}, \times)$ est un morphisme de groupes.

Exercice 1.12 *On note $\mathbb{Q}_+^* = \mathbb{Q} \cap]0, +\infty[$. Montrer que les groupes $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$ ne sont pas isomorphes (*indication: utiliser le fait que $\sqrt{2} \notin \mathbb{Q}$*).*

Exercice 1.13 (Automorphismes intérieurs) *Soit G un groupe. Pour tout $a \in G$, on définit une application $\psi_a : G \to G$ en posant $\psi_a(x) = axa^{-1}$ pour tout $x \in G$.*

1. *Montrer que pour tout $a \in G$, ψ_a est un automorphisme de G. Tout automorphisme de cette forme est appelé automorphisme intérieur.*
2. *Montrer que l'application $\Psi : G \to \mathrm{Aut(G)}$ qui à tout élément a de G associe ψ_a est un morphisme de groupes.*
3. *Montrer que l'ensemble* $\mathrm{Int(G)}$ *des automorphismes intérieurs forme un sous-groupe distingué de* $\mathrm{Aut(G)}$.
4. *Montrer que le centre $Z(G)$ de G est un sous-groupe distingué de G.*

2 Ordre d'un élément, ordre des sous-groupes, groupe quotient

2.1 Ordre d'un élément

Définition 2.1 *Soit $(G, \cdot)$ un groupe et soit x un élément de G. L'ordre de x est le plus petit entier $n \in \mathbb{N}^*$, s'il existe, tel que $x^n = 1$. Sinon, on dit que x est d'ordre infini.*

Autre définition : l'*ordre* de x est l'ordre du sous-groupe de G engendré par x.
(Rappel : l'*ordre* d'un groupe H est par définition son cardinal, on le note $|H|$).

Remarques : 0. Dans un groupe fini, tout élément est d'ordre fini.
1. Il existe des groupes infinis dans lesquels tout élément est d'ordre fini.
2. Il existe des groupes infinis engendrés par un nombre fini d'éléments d'ordre fini.
3. L'ordre des éléments est conservé par isomorphisme.

Proposition 2.2 *Soit $(G, \cdot)$ un groupe et soit x un élément de G. Alors pour tout $m \in \mathbb{N}^*$ on a : $x^m = 1$ si et seulement si l'ordre de x divise m.*

2.2 Groupes monogènes, groupes cycliques

Définition 2.3 *Un groupe est monogène s'il est engendré par un seul élément. Si de plus il est d'ordre fini, on dit que le groupe est cyclique.*

Remarques :
1. Un groupe cyclique est commutatif.
2. Les générateurs d'un groupe cyclique d'ordre n sont exactement ses éléments d'ordre n.

Théorème 2.4 *Soit $(G, \cdot)$ un groupe monogène. Alors:*
i) soit G est infini et est isomorphe à $(\mathbb{Z}, +)$.
ii) soit G est fini et G est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ où $n = |G|$.

Démonstration : Soit g un générateur de G. Si g est d'ordre infini, montrer que l'application $\varphi_g : (\mathbb{Z}, +) \to (G, \cdot)$ définie par $\varphi_g(k) = g^k$ est un isomorphisme. Si g est d'ordre fini n, montrer que l'application $\varphi_g : (\mathbb{Z}/n\mathbb{Z}, +) \to (G, \cdot)$ définie par $\varphi_g(\bar{k}) = g^k$ est bien définie et est un isomorphisme.

Les générateurs de $(\mathbb{Z}, +)$ sont 1 et -1.

Générateurs de $\mathbb{Z}/n\mathbb{Z}$

Proposition 2.5 *Soit $k \in \mathbb{Z}$. Alors $\bar{k}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$ ssi $k \wedge n = 1$.*

Conséquence : il y a $\varphi(n)$ générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$, où φ désigne l'indicateur d'Euler.

Corollaire 2.6 *Soit $(G, \cdot)$ un groupe cyclique d'ordre n et g un générateur de G. Alors les générateurs de G sont les g^k avec $k \wedge n = 1$.*

Démonstration : L'isomorphisme φ_g défini plus haut envoie un générateur sur un générateur.

Exercice 2.7 *Soit $(G,\cdot)$ un groupe cyclique d'ordre n et g un générateur de G. Alors pour tout $k \in \mathbb{N}$, l'ordre de g^k est $\frac{n}{k \wedge n}$.*

Exercice 2.8 (Groupes d'ordre 4) *Montrer que tout groupe d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

2.3 Classes, indice, théorème de Lagrange

Soit $(G,\cdot)$ un groupe et H un sous-groupe de G. La relation $\mathcal{R}_g$ définie sur G par :

$$x\mathcal{R}_g y \Leftrightarrow x^{-1}y \in H$$

est une relation d'équivalence.
Pour tout $x \in G$, $xH = \{xh, h \in H\}$ est la classe d'équivalence de x par $\mathcal{R}_g$ et s'appelle la *classe à gauche* de x. Toutes les classes à gauche ont même cardinal (celui de H) et elles forment une partition de G. On note $[G : H]$ le nombre de classes à gauche (appelé *indice* de H dans G). On a alors $|G| = [G : H] \times |H|$ et on en déduit le :

Théorème 2.9 (Théorème de Lagrange) *Soit G un groupe fini et H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G. En particulier l'ordre de tout élément de G divise l'ordre de G.*

Corollaire 2.10 *Soit G un groupe d'ordre fini n. Alors pour tout $x \in G$, $x^n = 1$.*

Corollaire 2.11 *Tout groupe d'ordre premier est cyclique.*

De manière similaire, on peut définir sur G une relation d'équivalence $\mathcal{R}_d$ et les *classes à droite* associées Hx (pour tout $x \in G$). Il y en a autant que de classes à gauche mais elles ne définissent pas nécessairement la même partition de G.

Exemple : Dans le groupe symétrique $\mathcal{S}_3$, déterminer les classes à gauche et à droite pour le sous-groupe $H =< (1,2) >$ (engendré par la transposition $(1,2)$).

Le cas où les deux partitions sont les mêmes correspond au cas où H est distingué dans G :

Proposition 2.12 *Soit G un groupe et H un sous-groupe.*
Alors H est distingué dans G ssi $\forall x \in G, xH = Hx$ (ie les classes à gauche et à droite coïncident).

Corollaire 2.13 *Tout sous-groupe d'indice 2 est distingué.*

2.4 Groupe quotient

Théorème 2.14 *Soit $(G,\cdot)$ un groupe et soit H un sous-groupe de G.*
Alors les propositions suivantes sont équivalentes :

(i) H est distingué dans G,

(ii) La loi de composition sur G induit une loi de composition bien définie sur $(G/H)_g$ (ensemble des classes à gauche).

Si H est un sous-groupe distingué de G, les classes à gauche et à droite coïncident et on peut donc définir $G/H = (G/H)_g = (G/H)_d$. D'après le théorème on peut munir G/H de la loi induite par la loi de G (définie par $xH \cdot yH = xyH$ pour tout $x, y \in G$). $(G/H, \cdot)$ est le *groupe quotient* de G par H.

Remarques : l'élément neutre est la classe de 1_G (=H). On a $|G| = |G/H| \times |H|$.

On notera $\bar{x}$ plutôt que xH la classe de x. La projection canonique $\pi : G \to G/H$ définie par $\pi(x) = \bar{x}$ est un morphisme de groupes et son noyau est H. Ainsi on a la :

Proposition 2.15 *Soit G un groupe et soit H un sous-groupe de G.*
Alors H est distingué dans G ssi H est le noyau d'un morphisme de groupes défini sur G.

Exemples :
1. $(\mathbb{Z}/n\mathbb{Z}, +)$ est le groupe quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$.
2. $]0, +\infty[$ est un sous-groupe (distingué) de $(\mathbb{R}^*, \times)$ et on a $\mathbb{R}^*/]0, +\infty[= \{\overline{1}, \overline{-1}\}$, $\overline{1} =]0, +\infty[$ et $\overline{-1} =]-\infty, 0[$.

Proposition 2.16 *Soit $f : G \to G'$ un morphisme de groupes. Alors f induit par passage au quotient un isomorphisme de groupes entre $G/\ker f$ et Imf. En particulier on a $|G| = |Imf| \times |\ker f|$.*

Exemples :
1. L'application $f : (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$ définie par $f(t) = e^{2i\pi t}$ est un morphisme de groupes, qui induit un isomorphisme $\mathbb{R}/\mathbb{Z} \simeq S^1$.
2. L'application $N : (\mathbb{C}^*, \times) \to (\mathbb{R}^*, \times)$ définie par $N(z) = |z|$ est un morphisme de groupes. On a $\ker N = S^1$, $ImN =]0, +\infty[$ et $\mathbb{C}^*/\ker N = \mathbb{C}^*/S^1 \simeq]0, +\infty[$.
3. Le morphisme det : $GL_n(\mathbb{R}) \to \mathbb{R}^*$ induit un isomorphisme $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$.
4. Pour tout groupe G, on a un isomorphisme Int(G) $\simeq$ G/Z(G) (cf exercice 1.13).

Exercice 2.17 *1. Soit G un groupe où pour tout x, $x^2 = e$. Montrer que G est abélien.*

2. *Pour cette question et la suivante, on suppose que G est de plus un groupe fini non trivial. Montrer qu'alors G est d'ordre pair.*

3. *En déduire que l'ordre de G est une puissance de 2 (*indication: on raisonnera par récurrence sur l'ordre de G en considérant un quotient bien choisi*).*

Exercice 2.18 (Groupes d'ordre 6) *Le but de cet exercice est de montrer que les seuls groupes d'ordre 6 sont, à isomorphisme près, $\mathbb{Z}/6\mathbb{Z}$ et $\mathcal{S}_3$. Soit G un tel groupe.*

1. *Montrer que G admet des éléments d'ordre 2 et 3 (cf ex. 2.17).*

2. *Soit b un élément d'ordre 3 de G. Montrer que $\langle b \rangle$ est distingué.*

3. *Soit a un élément d'ordre 2 de G. Montrer que aba est égal à b ou b^2.*

4. *Si $aba = b$, montrer que ab est d'ordre 6 et conclure que $G \simeq \mathbb{Z}/6\mathbb{Z}$.*

5. *Si $aba = b^2$, on pose $c = ab$ et $d = ba$. Montrer que $G = \{e, a, b, b^2, c, d\}$ et écrire la table de G. Conclure que $G \simeq \mathcal{S}_3$.*

3 Le groupe symétrique

Soit $n \in \mathbb{N}^*$. $\mathcal{S}_n$ est par définition l'ensemble des bijections de l'ensemble $\{1, \ldots, n\}$. C'est un groupe pour la composition des applications, d'ordre $n!$, et non commutatif dès que $n \geq 3$. les éléments de $\mathcal{S}_n$ s'appellent des *permutations*.

Notation $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.

Attention, on écrit souvent $\sigma\sigma'$ pour $\sigma \circ \sigma'$.

3.1 Décomposition en cycles

Définition 3.1 *Soit $\sigma \in \mathcal{S}_n$ et soit $x \in \{1, \ldots, n\}$.*
On appelle orbite de x pour σ l'ensemble $\mathcal{O}_x = \{\sigma^k(x), k \in \mathbb{Z}\}$.

Lemme 3.2 *Soit $\sigma \in \mathcal{S}_n$. Les orbites pour σ forment une partition de $\{1, \ldots, n\}$.*

Démonstration : les orbites sont les classes d'équivalence pour la relation d'équivalence $\mathcal{R}$ sur $\{1, \ldots, n\}$ définie par : $x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{Z}, y = \sigma^k(x)$.

Définition 3.3 *Une permutation est un cycle si elle possède exactement une orbite non réduite à un élément. Cette orbite s'appelle le support du cycle. Son cardinal est la longueur du cycle.*
Un cycle de longueur 2 s'appelle une transposition.

Notation $(a_1 a_2 \ldots a_l)$ pour un cycle.

Lemme 3.4 *Deux cycles à supports disjoints commutent.*

Théorème 3.5 *Toute permutation ($\neq id$) se décompose en produit de cycles à supports disjoints et cette décomposition est unique à l'ordre des facteurs près.*

Application : calcul des puissances d'une permutation, de son ordre.

Exercice 3.6 *Quel est le plus petit n tel que $\mathcal{S}_n$ contienne un élément d'ordre 14?*

3.2 Conjugaison

Soit $c = (a_1 a_2 \ldots a_l)$ un cycle et σ une permutation quelconque de $\mathcal{S}_n$. Alors on a :

$$\sigma c \sigma^{-1} = (\sigma(a_1)\sigma(a_2)\ldots\sigma(a_l)).$$

Le conjugué d'un cycle est donc un cycle de même longueur.

Pour un produit de cycles $C = c_1 c_2 \ldots c_k$ on a :

$$\sigma C \sigma^{-1} = (\sigma c_1 \sigma^{-1})(\sigma c_2 \sigma^{-1}) \ldots (\sigma c_k \sigma^{-1}).$$

Ceci permet de montrer le théorème qui va suivre en ayant auparavant établi la notation suivante : pour $\sigma \in \mathcal{S}_n \setminus \{id\}$, on note $l(\sigma) = (l_1, \cdots, l_k)$, $l_1 \geq \ldots \geq l_k > 1$ les longueurs des cycles dans sa décomposition en cycles à supports disjoints. On pose $l(id) = 1$.

Théorème 3.7 *Soit $\sigma, \sigma' \in \mathcal{S}_n$. Alors σ et σ' sont conjugués dans $\mathcal{S}_n$ ssi $l(\sigma) = l(\sigma')$.*

Applications :

1) Parties génératrices de $\mathcal{S}_n$

Proposition 3.8 *1. $\mathcal{S}_n$ est engendré par les transpositions.*

2. $\mathcal{S}_n$ est engendré par les transpositions de type $(i, i+1)$.

3. $\mathcal{S}_n$ est engendré par les transpositions (12) et $(12\ldots n)$.

2) Centre de $\mathcal{S}_n$

Exercice 3.9 *1. Soit $\sigma \in \mathcal{S}_n$ et c un cycle de $\mathcal{S}_n$. Calculer $\sigma c \sigma^{-1}$.*

2. Soit σ un élément du centre de $\mathcal{S}_n$. Montrer que pour tous $1 \leq i, j \leq n$, σ préserve $\{i, j\}$.

3. En déduire le centre de $\mathcal{S}_n$, pour $n \geq 2$.

3.3 Signature

Définition 3.10 *Soit $\sigma \in \mathcal{S}_n$. On appelle signature de σ le nombre $\varepsilon(\sigma) = (-1)^{n-k}$ où k est le nombre d'orbites suivant σ. Si $\varepsilon(\sigma) = 1$, on dit que σ est paire, si $\varepsilon(\sigma) = -1$, on dit que σ est impaire.*

Proposition 3.11 (Signature d'un cycle) *Soit $c \in \mathcal{S}_n$ un cycle de longueur l. Alors $\varepsilon(c) = (-1)^{l-1}$. En particulier, toute transposition est impaire.*

Théorème 3.12 *$\varepsilon : \mathcal{S}_n \to \{-1, +1\}$ est un morphisme de groupes.*

Le *groupe alterné* $\mathcal{A}_n$ est le noyau de ε, c'est-à-dire l'ensemble des permutations paires de $\mathcal{S}_n$. C'est un sous-groupe distingué de $\mathcal{S}_n$ d'ordre $n!/2$.

Exemple : déterminer $\mathcal{A}_4$.

Exercice 3.13 *Dans le groupe $\mathcal{S}_7$ des permutations de $\{1, \ldots, 7\}$, considérons les éléments*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 1 & 7 & 3 & 4 & 2 \end{pmatrix} \text{ et } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 4 & 1 & 7 & 2 \end{pmatrix}$$

1. Décomposer σ et τ en produits de cycles à supports disjoints.

2. Ces deux éléments sont-ils conjugués ?

3. Quel est l'ordre de σ ? Quel est l'élément σ^{145} ?