Université Lyon 1
Math I Algèbre
Automne 2009

Chapitre IV: Groupes

I. Un **groupe** est un ensemble non vide G muni d'une loi de composition interne

$$\star : G \times G \to G : (x, y) \mapsto x \star y$$

qui est **associative**, à **neutre** et à **réciproques** (ou inverses), ce qui signifie

associative: quels que soient $x, y, z \in G$, $(x \star y) \star z = x \star (y \star z)$

à neutre: il existe un élément $e \in G$ tel que, quel que soit $x \in G$, $x \star e = e \star x = x$.

à réciproque: quel que soit $x \in G$, il existe un élément $x^{-1} \in G$ tel que $x \star x^{-1} = x^{-1} \star x = e$.

Le groupe G est dit **commutatif** ou **abélien** si quels que soient $x, x' \in G$, $x \star x' = x' \star x$.

Exemples importants:

(1) $(\mathbf{Z}, +)$. Le neutre est $0 \in \mathbf{Z}$ et le réciproque de $m \in \mathbf{Z}$ est $-m \in \mathbf{Z}$.
De même, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$, $(\mathbf{C}, +)$.

(2) $(\mathbf{Q} \setminus \{0\}, \times)$. Le neutre est 1 et le réciproque de $\frac{p}{q}$ est $\frac{q}{p}$.
De même $(\mathbf{R} \setminus \{0\}, \times)$ et $(\mathbf{C} \setminus \{0\}, \times)$.

(3) L'ensemble $S(X)$ des bijections $f : X \to X$ muni de la composition des applications $\circ$. Le neutre est l'application identité id_X et le réciproque de f est la bijection réciproque f^{-1}.

(4) Comme cas particulier de (3), l'ensemble des bijections $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ muni de la composition $\circ$ est appelé le groupe des **permutations** ou encore le groupe **symétrique**. Dans ce cas, on utilise la notation plus courte S_n au lieu de $S(\{1, 2, \ldots, n\})$.

Tout élément $\sigma \in S_n$ se représente par un tableau

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$$

La composition $\circ$ s'obtient alors par juxtaposition des tableaux, par exemple pour $n = 4$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ on a

$$\sigma \circ \sigma' = \begin{pmatrix} 3 & 2 & 1 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

II. Le cardinal d'un groupe G est appelé son **ordre** et est souvent noté $| G |$ au lieu de card (G).

Un groupe G est dit **fini** s'il est d'ordre fini.

Exemples importants de groupes finis:

(1) Le groupe des permutations S_n est d'ordre $n!$

(2) L'ensemble $U_n = \{z \in \mathbf{C},\, z^n = 1\}$ des racines $n-$ ièmes de l'unité muni de la multiplication de $\mathbf{C}$ est un groupe d'ordre n. Explicitement on a

$$U_n = \{e^{\frac{2\pi ik}{n}},\, 0 \leq k \leq n-1\}$$

i.e. les racines $n-$ièmes de 1 sont les sommets d'un polygone régulier à n côtés inscrits sur le cercle unité $\{z \in \mathbf{C},\, \mid z \mid = 1\}$ du plan complexe.

(3) L'ensemble $\mathbf{Z}/n\mathbf{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ des classes de restes pour la division euclidienne par n est un groupe pour la loi d'addition

$$\overline{a} + \overline{a'} = \overline{a + a'}.$$

Le neutre est la classe $\overline{0}$ et le réciproque de la classe $\overline{a}$ est la classe $\overline{-a} = \overline{n-a}$.

La table de composition d'un groupe fini $G = \{x_0, x_1, \ldots, x_{n-1}\}$ d'ordre n (de loi $\star$ et de neutre x_0) est un tableau de n lignes et n colonnes dont l'élément situé dans la case (i, j) est $x_i \star x_j$.

Voici quelques exemples de tables de composition:

- table du groupe S_2:

$$\begin{array}{c|cc} \circ & id & t \\ id & id & t \\ t & t & id \end{array}$$

où

$$id = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

- table du groupe multiplicatif U_3:

$$\begin{array}{c|cccc} \times & 1 & e^{\frac{2\pi i}{3}} & e^{\frac{4\pi i}{3}} \\ 1 & 1 & e^{\frac{2\pi i}{3}} & e^{\frac{4\pi i}{3}} \\ e^{\frac{2\pi i}{3}} & e^{\frac{2\pi i}{3}} & e^{\frac{4\pi i}{3}} & 1 \\ e^{\frac{4\pi i}{3}} & e^{\frac{4\pi i}{3}} & 1 & e^{\frac{2\pi i}{3}} \end{array}$$

- table du groupe S_3:

$$\begin{array}{c|cccccc} \circ & id & c & c' & t_{12} & t_{13} & t_{23} \\ id & id & c & c' & t_{12} & t_{13} & t_{23} \\ c & c & c' & id & t_{13} & t_{23} & t_{12} \\ c' & c' & id & c & t_{23} & t_{12} & t_{13} \\ t_{12} & t_{12} & t_{23} & t_{13} & id & c' & c \\ t_{13} & t_{13} & t_{12} & t_{23} & c & id & c' \\ t_{23} & t_{23} & t_{13} & t_{12} & c' & c & id \end{array}$$

où

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad c' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$t_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad t_{13} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad t_{23} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

III. Soit G un groupe de loi $\star$ et de neutre $e \in G$.
Un **sous-groupe** K de G est une partie $K \subset G$ telle que

- $\forall k, k' \in K,\ k \star k' \in K$

- $e \in K$

- $\forall k \in K,\ k^{-1} \in K$.

Un sous-groupe K de G est dit **distingué** si quels que soient $k \in K$ et $x \in G$ on a $x \star k \star x^{-1} \in K$.

Exemples de sous-groupes

(1) $\mathbf{Q} \setminus \{0\}$ est un sous-groupe de $\mathbf{C} \setminus \{0\}$ pour la multiplication complexe.

(2) le groupe multiplicatif U_n des racines $n-$ ièmes de l'unité est un sous-groupe de $\mathbf{C} \setminus \{0\}$ pour la multiplication complexe.

(3) U_4 est un sous-groupe de U_8.

(4) (cf la table plus haut) $\{id, t_{ij}\}, i < j$ et $\{id, c, c'\}$ sont des sous-groupes du groupe de permutations S_3.

(5) quelquesoit $d \in \mathbf{N}$, la partie $d\mathbf{Z} = \{dl,\ l \in \mathbf{Z}\}$ est un sous-groupe de $\mathbf{Z}$ (pour l'addition). De plus on a la propriété suivante: pour tout sous-groupe K de $\mathbf{Z}$ il existe $d \in \mathbf{N}$ tel que $K = d\mathbf{Z}$; lorsque $K \neq \{0\}$, on a $d = \min\,(K \cap \mathbf{N} \setminus \{0\})$.

IV. Soient $(G, \star)$ et $(G', \star')$ deux groupes de neutres e et e'.
Une application $f : G \to G' : x \mapsto f(x)$ est appelée un **morphisme** si

$$\forall x, y \in G, \quad f(x \star y) = f(x) \star' f(y).$$

Tout morphisme satisfait $f(e) = e'$ et $f(x^{-1}) = (f(x))^{-1}$.
Un morphisme bijectif est appelé un **isomorphisme**.

Exemples de morphismes:

(1) L'application exponentielle

$$exp : \mathbf{R} \to \mathbf{R}_{>0} : x \mapsto exp(x)$$

satisfait, pour tous réels x, x',

$$exp(x + x') = exp(x)exp(x')$$

i.e. *exp* est un morphisme du groupe additif $(\mathbf{R}, +)$ vers le groupe multiplicatif $(\mathbf{R}_{>0}, \times)$. De plus, *exp* est un isomorphisme de bijection réciproque l'application logarithme ln.

(2) L'application

$$\mathbf{R} \to \mathbf{C} \setminus \{0\} : \theta \mapsto e^{i\theta} = cos\,\theta + i\,sin\,\theta$$

satisfait, pour tous réels θ, θ',

$$e^{i(\theta+\theta')} = e^{i\theta}e^{i\theta'}$$

i.e. c' est un morphisme de $(\mathbf{R}, +)$ vers $(\mathbf{C} \setminus \{0\}, \times)$.

(3) L'application

$$f : U_3 \to S_3$$
$$f(1) = id, \quad f(e^{\frac{2\pi i}{3}}) = c, \quad f(e^{\frac{4\pi i}{3}}) = c'$$

est un morphisme du groupe multiplicatif U_3 vers S_3.

(4) (cf tds) Il n'y a à isomorphisme près qu'un seul groupe d'ordre 3 i.e. tout groupe à trois éléments est isomorphe à $(U_3, \times)$.

(5) (cas particulier de (4)) L'application $f : \mathbf{Z}/3\mathbf{Z} \to U_3$ définie par

$$f(\overline{0}) = 1, \quad f(\overline{1}) = e^{\frac{2\pi i}{3}}, \quad f(\overline{2}) = e^{\frac{4\pi i}{3}}$$

est un isomorphisme du groupe additif $\mathbf{Z}/3\mathbf{Z}$ sur le groupe multiplicatif U_3. Pour le voir, écrire les tables de compositions de $\mathbf{Z}/3\mathbf{Z}$ et de U_3 et observer que l'application f transforme la première table en la seconde.

Soit $f : G \to G'$ un morphisme. On appelle **noyau** de f la partie

$$Ker\, f = \{x \in G,\ f(x) = e'\} \subset G$$

On appelle **image** de f la partie

$$Im\, f = \{f(x),\ x \in G\} \subset G'$$

Propriétés: $Ker\, f$ est un sous-groupe distingué de G. $Im\, f$ est un sous-groupe de G'.

Proposition: Un morphisme $f : G \to G'$ est injectif ssi $Ker\, f = \{e\}$.

V. Le théorème de Lagrange: Soit G un groupe fini et K un sous-groupe de G. Alors l'ordre (i.e. le cardinal) de K est un diviseur de l'ordre de G.

Ce théorème est important en pratique:

exemples:

(1) Les sous-groupes de S_3 sont d'ordre $1, 2, 3, 6$. Le sous-groupe d'ordre 1 est bien sûr $\{id\}$ et celui d'ordre 6 est S_3 lui-même. Les sous-groupes d'ordre 2 sont les $\{id, t_{ij}\}, i < j$ et le seul sous-groupe d'ordre 3 est $\{id, c, c'\}$ (cf plus haut).

(2) Si l'ordre de G est un nombre premier p, les seuls sous-groupes de G sont $\{e\}$ et G.

La preuve du théorème de Lagrange est elle aussi importante. Elle utilise la relation d'équivalence sur G définie par

$$a\, R\, b \Leftrightarrow a^{-1} \star b \in K$$

dont les classes

$$\overline{a} = a \star K = \{a \star h,\ h \in K\}$$

sont appelées les $K-$ **classes à gauche**.

VI. Sous-groupe engendré par un élément

Soit $(G, \star)$ un groupe de neutre e et a un élément de G.

Par associativité de la loi $\star$ on a

$$(a \star a) \star a = a \star (a \star a) \qquad (\star_3)$$

On peut dès lors *oublier* les parenthèses et noter a^3 la valeur commune de l'expression $(\star_3)$. Plus généralement pour $m \in \mathbf{N} \setminus \{0\}$, on écrit

$$a^0 = e, \quad a^m = a \star a^{m-1}, \quad a^{-m} = (a^{-1})^m.$$

On a , quels que soient $k, l \in \mathbf{Z}$,

$$a^k \star a^l = a^{k+l}.$$

Attention: lorsque la loi de groupe est additive (par exemple ($\mathbf{Z}$,+)) la notation signifie

$$a^0 = 0, \quad a^m = a + \cdots + a \ (m \text{ fois }) \quad a^{-m} = -a + \cdots + (-a) \ (m \text{ fois }).$$

On dit que $a \in G$ est **d'ordre infini** si pour tout $m \in \mathbf{N} \setminus \{0\}$ on a $a^m \neq e$.
Si a n'est pas d'ordre infini, on appelle **ordre** de a le plus petit entier n strictement positif tel que $a^n = e$.

Théorème: L'ensemble

$$< a >= \{a^n, \quad n \in \mathbf{Z}\} \subset G$$

est un sous-groupe de G dont l'ordre est égal à l'ordre de a.

La proposition qui suit résulte du théorème de Lagrange:

Corollaire: Soit G un groupe fini de neutre e. Quelquesoit $a \in G$ on a

$$a^{|G|} = e.$$

Un sous-groupe K de G est dit **monogène** s'il existe $a \in G$ tel que $K =< a >$. a est alors appelé un **générateur** de K.
Un sous-groupe K monogène et fini est dit **cyclique**.

Exemples:

(1) L'ensemble $2\,\mathbf{Z}$ des entiers pairs est un sous-groupe monogène de $(\mathbf{Z}, +)$ de générateur 2, i.e. $< 2 >_+ = 2\,\mathbf{Z}$.

(2) Le groupe U_n des racines $n-$ ièmes de 1 dans $\mathbf{C}$ est un groupe cyclique d'ordre n de générateur $e^{\frac{2\pi i}{n}}$ car

$$(e^{\frac{2\pi i}{n}})^l = e^{\frac{2\pi i l}{n}}.$$

(3) $e^{\frac{i\pi}{2}}$ est d'ordre 4 dans U_4 et $< e^{\frac{i\pi}{2}} >= U_4$.
$e^{i\pi}$ est d'ordre 2 dans U_4 et $< e^{i\pi} >= \{1, e^{i\pi} = -1\}$.

(4) Dans le groupe $(\mathbf{Z}/8\mathbf{Z}, +)$ la classe $\overline{2}$ est d'ordre 4: en effet

$$\overline{2} + \overline{2} = \overline{4}, \quad \overline{2} + \overline{2} + \overline{2} = \overline{6}, \quad \overline{2} + \overline{2} + \overline{2} + \overline{2} = \overline{8} = \overline{0}$$

et le sous-groupe engendré par $\overline{2}$ est dès lors

$$< \overline{2} >_+ = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$$

La classe $\overline{4}$ est d'ordre 2 dans $\mathbf{Z}/8\mathbf{Z}$ et $< \overline{4} >_+ = \{\overline{0}, \overline{4}\}$.
La classe $\overline{3}$ est d'ordre 8 et dès lors $< \overline{3} >_+ = \mathbf{Z}/8\mathbf{Z}$.

Plus généralement, on appelle **sous-groupe engendré** par une partie $P \subset G$ le plus petit sous-groupe $< P >\subset G$ contenant P. $< P >$ est l'intersection de tous les sous-groupes de G contenant P. Le cas plus haut correspond à $P = \{a\}$.