Université Lyon 1
Math I Algèbre
Automne 2010

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 $x \star e = e \star x = x$ quel que soit $x \in G$.

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 $x \star x' = x' \star x$ quels que soient $x, x' \in G$.

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

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

(3) L'ensemble $S(E)$ des bijections $f : E \to E$ de l'ensemble E, muni de la composition des applications $\circ$. Le neutre est l'application identité id_E 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 $\mathcal{S}_n$ au lieu de $S(\{1, 2, \ldots, n\})$.
Tout élément $\sigma \in \mathcal{S}_n$ 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 $\mid G \mid$ 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) Soit $n \in \mathrm{N} \setminus \{0\}$. L'ensemble $U_n = \{z \in \mathrm{C},\, z^n = 1\}$ des racines $n-$ ièmes de l'unité muni de la multiplication complexe $\times$ est un groupe d'ordre n.

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

$$\overline{a} + \overline{b} = \overline{a+b}, \quad a, b \in \mathrm{Z}.$$

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

Table d'un groupe fini:

Soit $(G = \{x_0, x_1, \ldots, x_{n-1}\}, \star)$ un groupe fini de neutre x_0. La table de composition de G est le tableau à n lignes et n colonnes dont l'élément (i,j) est $x_i \star x_j$:

$$\begin{array}{c|cccccc}
\star & x_0 & x_1 & \cdots & x_j & \cdots & x_{n-1} \\
x_0 & & & & & & \\
x_1 & & & & & & \\
\vdots & & & & & & \\
x_i & & & & x_i \star x_j & & \\
\vdots & & & & & & \\
x_{n-1} & & & & & &
\end{array}$$

Exemples: Voici la table de multiplication de $U_2 = \{+1, -1\}$:

$$\begin{array}{c|cc}
\times & 1 & -1 \\
1 & 1 & -1 \\
-1 & -1 & 1
\end{array}$$

Voici la table de multiplication de $U_3 = \{1, \omega = e^{\frac{2\pi i}{3}}, \omega^2\}$:

$$\begin{array}{c|ccc}
\times & 1 & \omega & \omega^2 \\
1 & 1 & \omega & \omega^2 \\
\omega & \omega & \omega^2 & 1 \\
\omega^2 & \omega^2 & 1 & \omega
\end{array}$$

Voici la table d'addition de $\mathrm{Z}/4\mathrm{Z}$:

$$\begin{array}{c|cccc}
+ & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\
\overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\
\overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{0} \\
\overline{2} & \overline{2} & \overline{3} & \overline{0} & \overline{1} \\
\overline{3} & \overline{3} & \overline{0} & \overline{1} & \overline{2}
\end{array}$$

Voici la table de composition 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

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

Propriété de la table d'un groupe fini:

- Chaque élément d'un groupe fini G figure une et une seule fois dans chaque ligne et chaque colonne de la table de G -

Démo: On le fait pour les lignes.
Supposons $x_i \star x_j = x_i \star x_k$. On a alors $x_i^{-1} \star (x_i \star x_j) = x_i^{-1} \star (x_i \star x_k)$ ou encore, par associativité, $(x_i^{-1} \star x_i) \star x_j = (x_i^{-1} \star x_i) \star x_k$. D'où $x_0 \star x_j = x_0 \star x_k$, i.e. $x_j = x_k$.
Dès lors pour $i, j \neq k$ on a $x_i \star x_j \neq x_i \star x_k$. Il y a donc n éléments distincts de G dans chaque ligne. Comme G a n éléments, chacun d'entre eux doit figurer une et une seule fois dans chaque ligne de la table.

Proposition:

- A notation et à permutation des éléments près, il y a une unique table de groupe d'ordre 2 et d'ordre 3 et il y a deux tables de groupe d'ordre 4 -

Je ne reprends pas la preuve complète dans ces notes. Pour 2 et 3, voir les exemples U_2 et U_3. Pour 4, la première table est celle de U_4 (ou celle de Z/4Z décrite plus haut) et la seconde est celle de $U_2 \times U_2$ pour la loi de groupe $(u, u') \cdot (v, v') = (uu', vv')$.

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

- $\forall h, h' \in K$, $h \star h' \in K$
- $e \in K$
- $\forall h \in K$, $h^{-1} \in K$.

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

Exemples de sous-groupes

(1) Q $\setminus \{0\}$ est un sous-groupe de C $\setminus \{0\}$ muni de $\times$.

(2) L'ensemble U_n des racines $n-$ ièmes de l'unité est un sous-groupe de C $\setminus \{0\}$ muni de $\times$.

(3) (cf la table plus haut) $\{id, t_{ij}\}, i < j$ et $\{id, c, c'\}$ sont des sous-groupes du groupe de permutations $\mathcal{S}_3$.

Sous-groupes de $(\mathrm{Z}, +)$:
Proposition: tout sous-groupe $K \subset \mathrm{Z}$ est de la forme

$$K = d\mathrm{Z} = \{dl,\, l \in \mathrm{Z}\}$$

pour un entier $d \in \mathrm{N}$.

Démo: cf Amphi.

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

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

Propriété: 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

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

satisfait

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

L'application f est donc un morphisme de $(\mathrm{R}, +)$ vers $(\mathrm{C} \setminus \{0\}, \times)$.
(2) 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 de $(U_3, \times)$ vers $(S_3, \circ)$.

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

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

Proposition: Un morphisme $f : G \to G'$ est injectif ssi $Ker\, f = \{e\}$.
Démo: supposons f injectif. Par la propriété plus haut, pour tout morphisme on a $f(e) = e'$. Par injectivité, si $f(x) = e' = f(e)$ alors $x = e$. (Sinon e' aurait 2 antécédents par f.)
Supposons $Ker\, f = \{e\}$.
Soient $x, x' \in G$ tels que $f(x) = f(x')$. On a

$$e' = (f(x))^{-1} \star' f(x) = (f(x))^{-1} \star' f(x') = f(x^{-1}) \star' f(x') = f(x^{-1} \star x').$$

Dès lors, $x^{-1} \star x' \in Kerf$, i.e. $x^{-1} \star x' = e$ ce qui équivaut à $x' = x$.

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

$\star\star$ **Ce qui suit n'a pas été traité en Amphi et ne figure donc pas au programme.** $\star\star$

V. Le théorème de Lagrange: Soit G un groupe fini et K un sous-groupe de G. Alors l'ordre 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 $\mathcal{S}_3$ 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

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

s'appellent les **classes à gauche**.

VI. Sous-groupe engendré par un élément

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

Pour $m \in \mathrm{N} \setminus \{0\}$, on écrit

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

On a

$$a^k \star a^l = a^{k+l}, \qquad \text{quels que soient } k, l \in \mathrm{Z}.$$

On dit que $a \in G$ est **d'ordre infini** si pour tout $m \in \mathrm{N} \setminus \{0\}$ 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

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

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

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 $2\,\mathrm{Z}$ des entiers pairs est un sous-groupe monogène de $(\mathrm{Z}, +)$ de générateur 2.

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

(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 $< e^{i\pi} >= \{1, e^{i\pi}\}$.

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 $P = \{a\}$.