L1S2 INFORMATIQUE — UNIVERSITÉ DE TOURS
Notes de Cours 2018-2019
Emmanuel Chasseigne

COURS NUMÉRO 4 — *Groupes, morphismes de groupes*

(a) Structure de groupe

Définition — Soit $(E, \star)$ un ensemble muni d'une lci. On dit que $(E, \star)$ est un groupe si les propriété suivantes sont satisfaites:

- La loi $\star$ est associative.
- $(E, \star)$ possède un élément neutre.
- Tout élément de E est symétrisable pour la loi $\star$.

On dit que le groupe est *Abélien* si la lci est également commutative.

En général on note e l'élément neutre (qui est unique), mais dans le cas d'un groupe additif, on peut le noter 0. On peut aussi le noter 1 dans le cas d'un groupe multiplicatif. L'élément symétrique est noté x^{-1}, mais aussi $-x$ (pour l'addition) et $1/x$ pour la multiplication.

Exemples: $(\mathbb{Z}, +)$, $(\mathbb{Q}, \times)$ etc...
Attention, $(\mathcal{P}(E), \cup)$ n'est pas un groupe même si on a bien une lci et un élément neutre.

(b) Règles de calcul dans un groupe

- $a \star x = a \star y \Rightarrow x = y$.
- $a \star x = b$ a une unique solution, $x = a^{-1}b$ (attention au cas non Abélien).
- Convention: $a^n = a \star a \star \dots a$; $a^n = e$.

(c) Sous-groupes

Définition — Soit $(E, \star)$ un groupe. On dit que F est un sous-groupe de $(E, \star)$ si:

- $\forall a, b \in F,\ a \star b \in F$
- $\forall a \in F,\ a^{-1} \in F$.

(stabilité par la lci et le passage à l'inverse).

Critère du sous-groupe:
F est un sous-groupe de $(E, \star)$ si pour tout $a, b \in F$, on a $a \star b^{-1} \in F$.

Exemples:
$n\mathbb{Z} := \{nz : z \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$.
$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{C}, +)$.

(d) Sous-groupe engendré par un élément

Définition — Soit $(E, \star)$ un groupe et $a \in E$. On note $< a >$ l'ensemble suivant: $< a > := \{a^n : n \in \mathbb{Z}\}$. Il s'agit d'un sous-groupe de $(E, \star)$ appelé sous-groupe engendré par a. On appelle ordre de a le plus petit entier $n > 0$ tel que $a^n = e$.

Par exemple, $n\mathbb{Z} =< n >$ dans $(\mathbb{Z}, +)$.

Théorème — Soit $(E, \star)$ un groupe d'ordre fini n. Alors l'ordre de tout sous-groupe est un diviseur de n. En particulier, l'ordre de tout élément divise l'ordre du groupe.

(e) Groupe des permutations

Soit E un ensemble quelconque de cardinal fini, n. Pour ce qui suit, on pourra considérer pour simplifier que $E = E_n = \{1, 2, ..n\}$.

Définition — Une permutation de E est une application $\sigma : E \to E$ qui est bijective. On dénote par $\mathcal{S}_n$ l'ensemble des permutations de E.

Proposition — $(\mathcal{S}_n, \circ)$ est un groupe d'ordre $n!$ appelé groupe symmétrique. Ce groupe n'est abélien que si $n \leq 2$.

Etant donné une permutation σ, la convention est de la noter ainsi:

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

On peut vérifier la non-commutativité dans $\mathcal{S}_3$ sur l'exemple suivant:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Définition — On appelle support d'une permutation σ l'ensemble des entiers i tels que $\sigma(i) \neq i$. Evidemment, $\mathrm{supp}\,(Id) = \emptyset$.

Proposition — Deux permutations de support disjoint commutent.

Il existe un certain nombre de permutation particulières:

Définition — On appelle transposition toute permutation $\sigma = \tau_{ij}$ qui ne fait que permuter i et j entre eux. On appelle p-cycle toute permutation telle que il existe $i_1, i_2, ...i_p$ tels que $\sigma(i_k) = i_{k+1}$ pour tout $k < p$ et $\sigma(i_p) = i_1$.

En particulier, une transposition est un 2-cycle, et le support d'un cycle est exactement $i_1, i_2, ... i_p$.

Théorème — Toute permutation σ se décompose en un produit de cycles. La décomposition est de plus unique si prend des cycles à supports disjoints.

(f) Ensembles d'entiers modulo p

Définition — Etant donné un entier $p \geq 2$, on note $\mathbb{Z}_p := \{\bar{0}, \bar{1}, \ldots \overline{p-1}\}$. Dire que $x \in \bar{0}$ signifie que x est un multiple de p. De même, par exemple,

$$x \in \bar{3} \iff x \equiv 3\,[\bmod p] = 3 + pk \iff x \in 3 + p\mathbb{Z}\,.$$

On peut munir $\mathbb{Z}_p$ d'une structure de groupe pour l'opération d'addition ainsi: $\bar{x} + \bar{y} = \overline{x+y}$. Par exemple, dans $\mathbb{Z}_4$,

$$\bar{2} + \bar{3} = \bar{5} = \bar{1}\,.$$

On peut ainsi établir sans difficulté la table de Cayley du groupe additif donc $\bar{0}$ est l'élément neutre et on voit par exemple que le symétrique de $\bar{2}$ est $\bar{2}$ lui-même pour ce groupe.

On peut s'intéresser aussi à la lci $\times$ en définissant $\bar{x} \times \bar{y} = \overline{xy}$, mais il est facile de voir qu'en général on n'a pas une structure de groupe pour cette loi, même en enlevant $\bar{0}$. Il faut que p soit premier pour qu'on ait une structure de groupe multiplicatif.

On renvoit aux TD pour plus de calculs sur ces groupes particuliers.

(g) Morphismes de groupes

Définition — Soient $(E, \star)$ et $(F, \perp)$ deux groupes. On dit que φ est un morphisme de groupe si

$$\forall (x,y) \in E^2\,, \quad \varphi(x \star y^{-1}) = \varphi(x) \perp (\varphi(y))^{-1}\,.$$

Si φ est bijective, on parle d'isomorphisme.

On s'intéresse de plus à deux objets:

Définition — Soit $\varphi : (E, \star) \to (F, \perp)$ un morphisme de groupes. On définit alors

- $\mathrm{Ker}(\varphi) := \{x \in E : \varphi(x) = e_F\}$.
- $\mathrm{Im}(\varphi) := \varphi(E)$.

Proposition — Soit $\varphi : (E, \star) \to (F, \perp)$ un morphisme de groupes. Alors

- $\text{Ker}(\varphi)$ est un sous-groupe de $(E, \star)$
- $\text{Im}(\varphi)$ est un sous-groupe de $(F, \perp)$
- φ est injectif si et seulement si $\text{Ker}(\varphi) = \{e_E\}$.

Exemple — Soit $n \in \mathbb{N}_*$. Alors l'application $\varphi(z) = nz$, définit un morphisme de groupe de $(\mathbb{Z}, +)$ dans lui-même, qui est injectif. Il n'est surjectif que si $n = \pm 1$.

Exercice — Démontrer que l'application ln est un morphisme du groupe $(]0, \infty[, \times)$ dans le groupe $(\mathbb{R}, +)$. On vérifiera d'abord qu'on a bien une structure de groupe pour chaque ensemble avec la lci correspondante.

(h) Structure de corps (introduction)

Définition — Soit un ensemble K muni de deux lci notées $+$ et $\times$. On dit que $(E, +, \times)$ est un corps si:

- $(E, +)$ est un groupe abélien.
- $(E_*, \times)$ est un groupe.
- la lci $\times$ est distributive sur la lci $+$.

Ici, E_* est l'ensemble E privé de l'élément neutre pour la lci $+$. En général, on note $0 = 0_E$ cet élément neutre, et on note $1 = 1_E$ l'élément neutre pour la lci $\times$. Donc $E_* = E \setminus \{0\}$. En particulier, dans un corps, tout élément différent de 0 admet un inverse.

Exemples — $(\mathbb{Q}, +, \times)$ est un corps, mais pas $(\mathbb{Z}, +, \times)$. De même, $(\mathbb{C}, +, \times)$ est un corps. On peut montrer que $(\mathbb{Z}_p, +, \times)$ est un corps à condition que p soit premier. Ce dernier est l'exemple typique d'un groupe ayant un nombre fini d'éléments.