Ecole Polytechnique
Formation préparatoire - EV2- Mathématiques

Résumé sur les groupes

1 Définitions

Un **groupe** est un ensemble $G \neq \emptyset$ muni d'une application de $G \times G$ dans G qui à (g_1, g_2) associe $g_1 g_2$ vérifiant les propriétés suivantes :
(i) $g_1(g_2 g_3) = (g_1 g_2) g_3$ (associativité)
(ii) il existe $e \in G$ tel que pour tout $g \in G$ on ait $eg = ge = g$ (e est l'élément neutre)
(iii) $\forall\, g \in G \quad \exists g^{-1} \in G \quad gg^{-1} = g^{-1}g = e$ (g^{-1} est l'inverse de g).

Exemples.
• L'ensemble des entiers $\mathbb{Z}$ muni de l'addition + est un groupe.
• L'ensemble des matrices inversibles de taille n (c'est-à-dire M de déterminant non nul) sur $\mathbb{R}$ (ou $\mathbb{C}$) muni de la multiplication est un groupe noté $Gl(n, \mathbb{R})$ (ou $Gl(n, \mathbb{C})$).
• L'ensemble $\mu_n = \{z \in \mathbb{C}, z^n = 1\} = \{e^{2i\pi k/n};\ k = 0, 1, \ldots n-1\}$ muni de la multiplication est un groupe
• $\mathbb{Z}^*$ muni de la multiplication n'est pas un groupe

Un groupe G est dit **commutatif** (ou **abélien**) si pour tout $(g, h) \in G \times G$ on a $gh = hg$. Très souvent dans ce cas, la loi du groupe est notée + (Exemple : $G = \mathbb{Z}$).

Si x et y sont dans G, on n'a pas toujours $(xy)^n = x^n y^n$. Cette égalité n'est vraie que lorsque $xy = yx$ (on dit x et y commutent).

Exemples. Les groupes $Gl(n, \mathbb{R})$ et $Gl(n, \mathbb{C})$ ne sont pas commutatifs pour $n \geq 2$, les autres exemples donnés sont des groupes commutatifs.

Un sous-groupe H de G est dit **distingué** (ou **normal**) si pour tout $x \in G$ et tout $h \in H$, on a $xhx^{-1} \in H$.

Un groupe est dit **simple** si ses seuls sous-groupes distingués sont $\{e\}$ et G.

2 Le groupe $\mathbb{Z}/n\mathbb{Z}$.

Soit $n \in \mathbb{N}$. On définit la relation d'équivalence $\sim$ sur $\mathbb{Z}$ par $x \sim y$ si et seulement si n divise $x - y$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence :

La classe d'équivalence d'un entier x est le sous-ensemble de $\mathbb{Z}$ formé des entiers de la forme $kn + x$ avec $k \in \mathbb{Z}$. Dans la suite, on représentera la classe d'équivalence de x par le reste $r \in \{0, \ldots n-1\}$ de la division euclidienne de x par n. On note également $x \bmod n$ la classe d'équivalence de x.

La loi de groupe sur $\mathbb{Z}/n\mathbb{Z}$ est définie par $(x \bmod n) + (y \bmod n) = (x + y) \bmod n$. Cette addition ne dépend pas du choix de x et de y dans la classe d'équivalence. En général, on écrit : dans $\mathbb{Z}/n\mathbb{Z}$, on a $x + y = \ldots$.

Exemple. Dans $\mathbb{Z}/21\mathbb{Z}$, on a $10 + 33 = 10 + 12 = 22 = 1$

Muni de cette loi, $\mathbb{Z}/n\mathbb{Z}$ est un groupe commutatif.

Bien sûr, on peut définir une loi multiplicative sur $\mathbb{Z}/n\mathbb{Z}$ en posant $(x \bmod n) \times (y \bmod n) = (xy) \bmod n$. L'ensemble $\mathbb{Z}/n\mathbb{Z} - \{0\}$ muni de cette loi n'est pas un groupe en général. On rappelle le résultat suivant :

Théorème de Bezout : Soit $k \in \mathbb{Z}$. Alors, k et n sont premiers entre eux si et seulement si il existe $(u, v) \in \mathbb{Z}^2$ tels que $uk + vn = 1$.

Ainsi, on a : $(\mathbb{Z}/n\mathbb{Z} - \{0\}, \times)$ est un groupe si et seulement si n est un nombre premier. Si n n'est pas premier, une classe n'a pas toujours d'inverse.

On note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ pour la loi $\times$. L'ensemble $(\mathbb{Z}/n\mathbb{Z})^*$ est formé des $x \in \mathbb{Z}/n\mathbb{Z}$ tels que x est premier avec n et $\big((\mathbb{Z}/n\mathbb{Z})^*, \times\big)$ est un groupe commutatif.

Exemple. On a $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ et $4 \times 4 = 1 \quad 3 \times 2 = 1$.

Dans $\mathbb{Z}/8\mathbb{Z}$, 4 n'a pas d'inverse pour la multiplication (on ne peut pas trouver x tel que $4x = 1 \bmod 8$).

Lemme Chinois : Si m et n sont premiers entre eux alors

$$(\mathbb{Z}/nm\mathbb{Z}, +) \simeq (\mathbb{Z}/n\mathbb{Z}, +) \times (\mathbb{Z}/m\mathbb{Z}, +) \qquad \big((\mathbb{Z}/nm\mathbb{Z})^*, \times\big) \simeq \big((\mathbb{Z}/n\mathbb{Z})^*, \times\big) \times \big((\mathbb{Z}/m\mathbb{Z})^*, \times\big).$$

3 Groupes cycliques.

Un groupe G est dit **cyclique** s'il existe $x_0 \in G$ tel que, pour tout $x \in G$, il existe $n \in \mathbb{Z}$ vérifiant $x = x_0^n$. On dit que x_0 est un **générateur** de G.

Exemples et propriétés.
1) $\mathbb{Z}$ est cyclique dont les générateurs sont 1 et -1. Un entier k positif s'écrit $k = \underbrace{1 + 1 + \ldots + 1}_{k \text{ fois}}$

2) $\mathbb{Z}/n\mathbb{Z}$ est cyclique, x est un générateur si et seulement si x est premier à n. En effet par le théorème de Bezout si x et n sont premiers entre eux, il existe u et v dans $\mathbb{Z}$ tels que $ux + nv = 1$ et donc $ux = 1 \bmod n$.

(Vérifier par vous-même ce résultat pour $n = 5$, $n = 6$ et $n = 12$.)

3) $\mu_n = \{z \in \mathbb{C}; z^n = 1\}$ est cyclique de générateurs $e^{2i\pi k/n}$ avec k premier à n.
4) Si G est cyclique, ses sous-groupes sont cycliques.
5) Si G est cyclique de cardinal n alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et pour tout d diviseur de n, il existe un unique sous-groupe H de G cyclique de cardinal d.

4 Groupes finis.

Un groupe **fini** est un groupe qui a un nombre fini n d'éléments. L'entier n est appelé le **cardinal** ou **l'ordre** de G. On note souvent $n = |G|$.

Soit G un groupe d'ordre fini $|G| = n$.

Théorème de Lagrange. si H est un sous-groupe de G alors $|G/H| \;\; |H| = |G|$.

L'ordre d'un élement x de G est le plus petit entier r tel que $x^r = e$.

Ne pas confondre l'ordre d'un groupe et l'ordre d'un élément du groupe : si x est d'ordre k alors le sous-groupe H engendré par x (c'est-à-dire le plus petit sous-groupe contenant x) est d'ordre k. On a $H = \{e, x, x^2, \ldots, x^{k-1}\}$.

Ainsi, par le théorème de Lagrange, **l'ordre d'un élément $x \in G$ divise l'ordre $|G|$ du groupe** G. En particulier, pour tout $x \in G$, on a $x^n = e$.

Exemples.
• Dans $(\mathbb{Z}/p\mathbb{Z}, +)$ avec p nombre premier, tout élément non nul est d'ordre p.
• Dans $\mathbb{Z}/12\mathbb{Z}$, on a 1 est d'ordre 12, 2 est d'ordre 6, 3 est d'ordre 4, 6 est d'ordre 2, 7 est d'ordre 12, 8 est d'ordre 3, 9 est d'ordre 4, 11 est d'ordre 12.

5 Morphisme de groupes.

Un **morphisme de groupes** entre deux groupes G et G' notés multiplicativement est une application $\varphi : G \to G'$ telle que
(a) pour tout x et y dans G l'on ait $\varphi(xy) = \varphi(x)\varphi(y)$
(b) $\varphi(e) = e'$.

Si de plus φ est bijective, on dit que φ est un isomorphisme (de groupes).

Si G est noté multiplicativement et G' additivement ces relations deviennent :
(a) pour tout x et y dans G l'on ait $\varphi(xy) = \varphi(x) + \varphi(y)$
(b) $\varphi(e) = 0$.

Remarques :
(1) On a $\varphi(x) = \varphi(y)$ si et seulement si $\varphi(xy^{-1}) = e$ et donc φ est injective si et seulement si le noyau de φ (noté $Ker(\varphi) = \{x \in G; \varphi(x) = e\}$) est $\{e\}$.
(2) si x est d'ordre k alors l'ordre de $\varphi(x)$ divise k.
Ainsi, il est facile de voir que $\mathbb{Z}/2Z \times Z/2Z$ et $\mathbb{Z}/4\mathbb{Z}$ ne sont pas isomorphes, dans le premier les éléments non nuls sont d'ordre 2, dans le second, l'élément 3 est d'ordre 4.

Exemples :

$$\begin{array}{rccc} \varphi : & \mathbb{Z}/n\mathbb{Z} & \to & \mu_n \\ & k & \to & e^{2i\pi k/n} \end{array}$$ est un isomorphisme de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans μ_n.

Si G est un groupe cyclique d'ordre n alors il existe $y \in G$ tel que $G = \{e, y, \dots y^{n-1}\}$. et dans ce cas

$$\begin{array}{rccc} \varphi : & \mathbb{Z}/n\mathbb{Z} & \to & G \\ & k & \to & y^k \end{array}$$ est un isomorphisme de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans G.

6 Le groupe symétrique.

Soit $n \in \mathbb{N} - \{0\}$. Le **groupe symétrique** S_n est l'ensemble des bijections de $\{1, \dots n\}$. Un élément de S_n est appelé **permutation**. Le **support** de $\sigma \in S_n$ est $\{i \in \{1, \dots n\}; \sigma(i) \neq i\}$.

Un **k-cycle** est une permutation τ telle qu'il existe $i_1, \dots i_k$ distincts vérifiant $\tau(i_1) = i_2, \tau(i_2) = i_3, \dots \tau(i_k) = i_1$ et $\tau(j) = j$ sinon. On le note $(i_1, i_2, \dots i_k)$.

Un 2-cycle est appelé une **transposition**.

La **signature** de τ est $sign(\tau) = \prod_{i \neq j} \frac{\tau(i) - \tau(j)}{i - j} \in \{-1, 1\}$ (on la note également $\epsilon(\tau)$). La signature est l'unique morphisme de groupes de S_n dans $\{\pm 1\}$.

Le **groupe altermé** A_n est le sous-groupe de S_n des permutations de signature 1.

Propriétés :
1) Deux permutations de supports disjoints commutent.
2) Une permutation est produit de cycles de support disjoints.
3) S_n est engendré par les transpositions.
4) A_n est engendré par les 3 cycles.
5) Pour $n \geq 5$ le groupe A_n est simple.

7 Action de groupe

Soit G un groupe et X un ensemble.
On dit que G opère (à gauche) sur X (ou encore " X est muni d'une action (à gauche) de G" ou encore G agit (à gauche) sur X") s'il existe une application $G \times X \to X$ qui à (g, x) associe $g.x$ telle que $e.x = x$ et $g.(g'.x) = (gg').x$.

On note $\sigma_g : X \to X$ l'application définie par $\sigma_g(x) = g.x$.
C'est une bijection de X et $g \to \sigma_g$ est morphisme de groupes de G dans l'ensemble des bijections de X muni de la composition.
L'orbite de $x \in X$ est l'ensemble $O_x = G.x = \{y \in X; \exists g \in G \ \ y = g.x\}$.
Le **stabilisateur** de $x \in X$ est le sous-groupe $G_x = \{g \in G; g.x = x\}$ de G.

L'application $g \to g.x$ induit une bijection de G/G_x dans O_x.

Si G est un groupe fini qui agit sur un ensemble fini X, on a **l'équation aux classes** :

$$|X| = \sum_{x \in G\backslash X} |O_x| = |G| \sum_{x \in G\backslash X} \frac{1}{|G_x|}$$

Exemple. La **classe de conjugaison** d'un élément $x \in G$ est l'orbite de x sous l'action de G sur lui-même par conjugaison : $(g, x) \to \sigma_g(x) = g \ x \ g^{-1}$. Le sous-groupe G_x est alors appelé le **centralisateur** de x.

A noter que la relation $x \sim y$ si et seulement si il existe $z \in G$ tel que $x = zyz^{-1}$ définit une relation d'équivalence sur G et les classes d'équivalence pour cette relation sont les classes de conjugaison.