Groupes finis

Quelques rappels

Sauf précision contraire, les groupes sont notés multiplicativement et on note 1 l'élément neutre.

- **Ordre d'un groupe.**
  Si $(G,\cdot)$ est un groupe ayant un nombre fini d'éléments son cardinal est appelé l'ordre de G.
- **Ordre d'un élément dans un groupe.**
  Si $(G,\cdot)$ est un groupe, pour tout g dans G, on note $\langle g\rangle = \left\{g^k \mid k\in\mathbb{Z}\right\}$ le sous groupe de G engendré par g.
  On rappelle que les puissances entières, positives ou négatives, de g sont définies par :

$$\begin{cases} g^0 = 1 \\ \forall n\in\mathbb{N},\ g^{n+1} = g^n g \\ \forall n\in\mathbb{N}^*,\ g^{-n} = \left(g^n\right)^{-1} \end{cases}$$

On peut remarquer que pour $n\in\mathbb{N}^*$, on a aussi $g^{-n} = \left(g^{-1}\right)^n$, ce qui résulte de :

$$\left(g^{-1}\right)^n g^n = g^{-1}\cdots g^{-1} g\cdots g = 1.$$

Si $\langle g\rangle$ est infini, on dit alors que g est d'ordre infini dans G, sinon on dit que g est d'ordre fini dans G et l'ordre de g est :

$$\theta(g) = \operatorname{card}\left(\langle g\rangle\right).$$

On a $\theta(g) = 1$ si, et seulement si, $g = 1$ et $\theta(g) = m \geq 2$ équivaut à dire que $g^m = 1$ et $g^k \neq 1$ pour tout k est compris entre 1 et $m-1$ ($\theta(g)$ est le plus petit entier naturel non nul tel que $g^m = 1$), ce qui est encore équivalent à dire que pour $k\in\mathbb{Z}$, on a $g^k = 1$ si, et seulement si, k est multiple de m. Tout cela est lié au théorème de division euclidienne dans $\mathbb{Z}$ et à la connaissance des sous-groupes additifs de $\mathbb{Z}$.

- **Groupes monogènes, cycliques.**
  On dit qu'un groupe $(G,\cdot)$ est monogène s'il existe $g\in G$ tel que $G = \langle g\rangle$. Si de plus, G est fini, on dit alors qu'il est cyclique.
- **Ensemble quotient G/H des classes à gauche modulo un sous-groupe H.**
  Soient $(G,\cdot)$ un groupe et H un sous-groupe.
  On rappelle que la relation $\sim$ définie sur G par :

$$g_1 \sim g_2 \Leftrightarrow g_1^{-1} g_2 \in H$$

  est une relation d'équivalence.
  Pour tout $g\in G$, on note $\overline{g}$ la classe d'équivalence de g et on dit que $\overline{g}$ est la classe à gauche modulo H de g. Précisément, on a :

$$\overline{g} = \{gh \mid h\in H\} = gH$$

  L'ensemble quotient G/H est l'ensemble des classes à gauche modulo H.
  L'application :

$$\begin{array}{rccc} \pi: & G & \to & G/H \\ & g & \mapsto & \overline{g} = gH \end{array}$$

  est surjective. On dit que c'est la surjection canonique de G sur G/H.
  On rappelle que l'ensembles des classes d'équivalences deux à deux distinctes forme une partition de G.
  Le cardinal de G/H est noté $[G:H]$ et appelé l'indice de H dans G, c'est un élément de $\mathbb{N}^*\cup\{+\infty\}$.

– **Sous-groupes distingués, groupe quotient.**
Un sous-groupe H de G est distingué (ou normal) si on a $gH = Hg$ pour tout $g \in G$, ce qui équivaut encore à dire que $ghg^{-1} \in H$ pour tout $(h, g) \in H \times G$.
Dans un groupe commutatif, tout sous-groupe est distingué.
On montre qu'un sous-groupe H de G est distingué si, et seulement si, il existe une unique structure de groupe sur l'ensemble quotient G/H des classes à gauche modulo H telle que la surjection canonique $\pi : G \to G/H$ soit un morphisme de groupes.
En particulier, pour G commutatif, G/H est un groupe.
Si G, G' sont deux groupes, φ un morphisme de groupes de G dans G', alors $\ker(\varphi)$ est un sous-groupe distingué de G et $G/\ker(\varphi)$ est un groupe isomorphe à $\mathrm{Im}(\varphi)$.
Dans le cas où G est fini, on en déduit que :

$$\mathrm{card}(G) = \mathrm{card}(\ker(\varphi))\,\mathrm{card}(\mathrm{Im}(\varphi))$$

Le centre $Z(G)$ (l'ensemble des éléments de G qui commutent à tous les autres éléments) est le noyau du morphisme de groupes $a \mapsto f_a : g \mapsto aga^{-1}$ de G dans $\mathrm{Aut}(G)$, c'est donc un sous-groupe distingué de G et $G/Z(G)$ est un groupe.

– **Actions de groupes.**
Si $(G, \cdot)$ est un groupe et X un ensemble non vide, on dit que G opère à gauche sur X si on a une application :

$$\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \mapsto & g \cdot x \end{array}$$

telle que :

$$\begin{cases} \forall x \in X,\ 1 \cdot x = x \\ \forall (g, g', x) \in G^2 \times X,\ g \cdot (g' \cdot x) = (gg') \cdot x \end{cases}$$

Une telle application est aussi appelée action à gauche de G sur X.
Un groupe G agit sur tout sous-groupe distingué H par conjugaison :

$$(g, h) \in G \times H \mapsto g \cdot h = ghg^{-1} \in H$$

Pour tout $x \in X$, on dit que le sous-ensemble de X :

$$G \cdot x = \{g \cdot x \mid g \in G\}$$

est l'orbite de x sous l'action de G.
On vérifie facilement que la relation $x \sim y$ si, et seulement si, il existe $g \in G$ tel que $y = g \cdot x$ est une relation d'équivalence sur X ($x = 1 \cdot x$ donne la réflexivité, $y = g \cdot x$ équivalent à $x = g^{-1} \cdot y$ donne la symétrie et $y = g \cdot x$, $z = h \cdot y$ qui entraîne $z = (hg) \cdot x$ donne la transitivité) et la classe de $x \in X$ pour cette relation est l'orbite de x. Il en résulte que les orbites forment une partition de X.
Pour tout $x \in X$, on dit que l'ensemble :

$$G_x = \{g \in G \mid g \cdot x = x\}$$

est le stabilisateur de x sous l'action de G. Ces stabilisateurs sont des sous-groupes de G (en général non distingués).
Pour tout $x \in X$, l'application $\overline{g} \in G/G_x \mapsto g \cdot x \in G \cdot x$ est bien définie et réalise une bijection de G/G_x sur $G \cdot x$ et pour G fini, on a :

$$\mathrm{card}(G \cdot x) = \frac{\mathrm{card}(G)}{\mathrm{card}(G_x)}$$

– **Indicateur d'Euler.**
Pour tout entier naturel $n \geq 2$, on note $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ l'anneau des classes résiduelles modulo n, $\mathbb{Z}_n^\times$ le groupe multiplicatif des éléments inversibles de cet anneau et $\varphi(n)$ le nombre d'éléments de $\mathbb{Z}_n^\times$ (indicateur d'Euler). On pose $\varphi(1) = 1$.
– Si p, q sont deux entiers relatifs, on note $p \wedge q$ le pgcd de p et q et $p \vee q$ le ppcm de p et q.

Généralités

1. Soient $(G, \cdot)$ un groupe fini d'ordre $n \geq 2$ et H un sous-groupe distingué de G. Comparer l'ordre de $\overline{g}$ dans G/H avec l'ordre de g dans G.
2. Montrer qu'un groupe G est fini si et seulement si l'ensemble de ses sous-groupes est fini.
3. Soit $(G, \cdot)$ un groupe tel que tout élément de G soit d'ordre au plus égal à 2.
   (a) Montrer que G est commutatif.
   (b) On suppose de plus que G est fini. Montrer qu'il existe un entier $n \geq 0$ tel que $\text{card}(G) = 2^n$.
4. Soit $\mathbb{K}$ est un corps de caractéristique différente de 2 et n un entier naturel non nul.
   (a) Montrer que si G est un sous-groupe multiplicatif fini de $GL_n(\mathbb{K})$ tel que tout élément de G soit d'ordre au plus égal à 2, alors est commutatif de cardinal inférieur ou égal à 2^n.
   (b) En déduire que pour $(n, m) \in (\mathbb{N}^*)^2$ les groupes multiplicatifs $GL_n(\mathbb{K})$ et $GL_m(\mathbb{K})$ sont isomorphes si, et seulement si, $n = m$.
5. Donner des exemples de groupes infinis dans lequel tous les éléments sont d'ordre fini.
6. Donner des exemples de groupes dans lequel on peut trouver deux éléments d'ordre fini dont le produit est d'ordre infini.

– I – Le théorème de Lagrange

1. Soient $(G, \cdot)$ un groupe fini et H un sous-groupe de G.
   (a) Montrer que pour tout $g \in G$, on a $\text{card}(gH) = \text{card}(H)$.
   (b) Montrer que :
   $$\text{card}(G) = [G : H]\,\text{card}(H)$$
   et en conséquence l'ordre de H divise celui de G (théorème de Lagrange).
   Prenant $H = \langle g \rangle$ avec $g \in G$, on déduit que l'ordre d'un élément g de G divise l'ordre de G.

   Avec les questions qui suivent, on donne quelques applications du théorème de Lagrange.
2. Montrer qu'un groupe de cardinal premier est cyclique (donc commutatif et isomorphe à $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, ce qui signifie qu'à isomorphisme près, il y a un seul groupe d'ordre p premier).
3. Déterminer les sous groupes finis de $(\mathbb{C}^*, \cdot)$.
4. Montrer que, pour tout entier $n \geq 1$, il existe un unique sous-groupe de $(\mathbb{Q}/\mathbb{Z}, +)$ d'ordre n.
5. Soient $(G, \cdot)$ un groupe et H, K deux sous-groupes distincts de G d'ordre un même nombre premier $p \geq 2$. Montrer que $H \cap K = \{1\}$.
6. Soient $(G, \cdot)$ un groupe, H un sous-groupe de G et K un sous-groupe de H. Montrer que si l'indice de K dans G est fini, alors l'indice de H dans G et celui de K dans H sont aussi finis et on a :
   $$[G : K] = [G : H]\,[H : K]$$

7. Soient g_1, g_2 deux éléments d'un groupe fini $(G, \cdot)$ d'ordres respectifs m_1 et m_2 tels que $g_1 g_2 = g_2 g_1$.
   (a) Montrer que si m_1 et m_2 sont premiers entre eux, alors $g_1 g_2$ est d'ordre $m_1 m_2$.
   (b) Si m_1 et m_2 ne sont pas premiers entre eux, $g_1 g_2$ est-il d'ordre $m_1 \vee m_2$?
   (c) Montrer qu'il existe dans G un élément d'ordre $m_1 \vee m_2$ (en utilisant les décompositions en facteurs premiers, on pourra écrire que $m_1 \vee m_2 = m_1' m_2'$, où m_1' et m_2' sont premiers entre eux et $m_1 = m_1' n_1$, $m_2 = m_2' n_2$).
8. Soit $(G, \cdot)$ un groupe commutatif, $p \geq 2$ un entier et $g_1, g_2, \cdots, g_p$ des éléments deux à deux distincts de G d'ordres respectifs $m_1, m_2, \cdots, m_p$. Montrer qu'il existe dans G un élément d'ordre égal au ppcm de ces ordres.
9. Soit $(G, \cdot)$ un groupe commutatif fini. Montrer que :
$$\max_{g \in G} \theta(g) = \text{ppcm}\{\theta(g) \mid g \in G\}$$
($\max_{g \in G} \theta(g)$ est l'exposant du groupe G).
10. Montrer qu'un groupe commutatif d'ordre pq, où p et q sont deux nombres premiers distincts, est cyclique.
11. Montrer que tout sous groupe fini du groupe multiplicatif $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ d'un corps commutatif $\mathbb{K}$ est cyclique.
12. Soit $n \geq 2$. Montrer que si k est un entier relatif premier avec n, alors $k^{\varphi(n)} \equiv 1 \pmod{n}$ (théorème d'Euler).
13. Montrer que pour $n \geq 3$, $\varphi(n)$ est un entier pair.
14. Montrer qu'un entier n est premier si et seulement si $(n-1)! \equiv -1 \ (n)$ (théorème de Wilson).
15. Soit p un nombre premier impair.
   (a) En utilisant l'application $x \mapsto x^2$ de $\mathbb{Z}_p^\times$ dans $\mathbb{Z}_p^\times$, montrer qu'il y a exactement $\dfrac{p-1}{2}$ carrés dans $\mathbb{Z}_p^\times$.
   (b) Montrer que l'ensemble des carrés de $\mathbb{Z}_p^\times$ est l'ensemble des racines du polynôme $P(X) = X^{\frac{p-1}{2}} - \overline{1}$.
   (c) En déduire que $\overline{(-1)}$ est un carré dans $\mathbb{Z}_p$ si, et seulement si, p est congru à 1 modulo 4.
   (d) En déduire qu'il existe une infinité de nombres premiers de la forme $4n+1$.
16. On appelle nombre de Fermat tout entier de la forme :
$$F_n = 2^{2^n} + 1$$
où n est un entier naturel.
On désigne par p un diviseur premier d'un nombre de Fermat F_n et on suppose que $p \neq F_n$.
   (a) Montrer que pour $n \neq m$ dans $\mathbb{N}$, F_n et F_m sont premiers entre eux.
   (b) Montrer que $p \geq 3$.
   (c) Montrer que $\overline{2}$ est d'ordre 2^{n+1} dans le groupe multiplicatif $\mathbb{Z}_p^*$.
   (d) Montrer que p congru à 1 modulo 2^{n+1}.
   (e) Soient $r \geq 1$ et $a \geq 2$ deux entiers. Montrer que si $a^r + 1$ est premier, alors a est pair et il existe un entier $n \geq 0$ tel que $r = 2^n$.

(f) Montrer que $p = 2^{n+1}q + 1$, où q est un entier qui admet un diviseur premier impair.
Pour $F_5 = 4\ 294\,967\,297$, s'il n'est pas premier ses diviseurs premiers sont de la forme $p = 2^6 q + 1 = 64q + 1$ où les valeurs possibles de q sont $3, 5, 6, 7, 9, 10, \cdots$ En essayant successivement ces valeurs, on aboutit à :

$$\frac{F_5}{641} = \frac{4\ 294\,967\,297}{641} = 6700\,417$$

et F_5 n'est pas premier (ce qui fût montré par Euler).

– II – Actions de groupes

1. Soit $(G, \cdot)$ est un groupe opérant sur un ensemble X.
On note X^G l'ensemble des éléments $x \in X$ tels que $G \cdot x = \{x\}$ (orbite réduite à un seul élément).

   (a) Montrer que pour tout $x \in X$ l'application :

$$\begin{array}{rccc} \varphi_x : & G/G_x & \to & G \cdot x \\ & \overline{g} = g \cdot G_x & \mapsto & g \cdot x \end{array}$$

   est bien définie et bijective.

   (b) On suppose que G et X sont finis et on note $G \cdot x_1, \cdots, G \cdot x_r$ toutes les orbites deux à deux distinctes. Montrer que :

$$\operatorname{card}(X) = \sum_{i=1}^{r} \operatorname{card}(G \cdot x_i) = \sum_{i=1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{x_i})}$$

   (formule des classes).

   (c) On suppose que X est fini et G fini de cardinal p^α, où p est un nombre premier et α un entier naturel non nul (on dit que G est un p-groupe). Montrer que :

$$\operatorname{card}\left(X^G\right) \equiv \operatorname{card}(X) \pmod{p}.$$

2. On rappelle que le centre d'un groupe $(G, \cdot)$, noté $Z(G)$, est l'ensemble des éléments de G qui commutent à tout élément de G.

   (a) Montrer que $Z(G)$ est un sous-groupe commutatif de G.

   (b) On suppose le groupe G fini et on le fait opère sur lui même par conjugaison ($g \cdot h = ghg^{-1}$, pour $(g, h) \in G \times G$). On note $G \cdot h_1, \cdots, G \cdot h_r$ toutes les orbites non réduites à un élément et deux à deux distinctes. Montrer que :

$$\begin{aligned} \operatorname{card}(G) &= \operatorname{card}(Z(G)) + \sum_{i=1}^{r} \operatorname{card}(G \cdot h_i) \\ &= \operatorname{card}(Z(G)) + \sum_{i=1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{h_i})}. \end{aligned}$$

   (c) Montrer que le centre d'un p-groupe n'est pas réduit à $\{1\}$.

3. On se propose de montrer que si G est un groupe d'ordre p^2 avec p premier, alors il est commutatif.

(a) On suppose que le centre $Z(G)$ du groupe G est de cardinal p et on se donne un élément $h \in G \setminus Z(G)$. Montrer que $Z(G) \cap \langle h \rangle = \{1\}$.

(b) Avec l'hypothèse de la question précédente, montrer que tout élément de G s'écrit de manière unique $g^i h^j$ où i, j sont des entiers compris entre 0 et $p-1$ et conclure.

– III – Le lemme de Cauchy

1. Soit $G = \langle a \rangle$ un groupe cyclique d'ordre $n \geq 2$.

   (a) Soit $g = a^k \in G$. Montrer que l'ordre de g est égal à $\dfrac{n}{n \wedge k}$.

   (b) Montrer que si H est un sous-groupe de G non réduit à $\{1\}$, alors $H = \langle a^p \rangle$ où p divise n et H est cyclique d'ordre $\dfrac{n}{p}$ (tout sous-groupe d'un groupe cyclique est cyclique).

   (c) Montrer que pour tout diviseur d de n, il existe un unique sous groupe de G d'ordre d, c'est le groupe cyclique $H = \langle a^p \rangle$ avec $p = \dfrac{n}{d}$.
   Réciproquement, on peut montrer qu'un groupe fini ayant cette propriété est nécessairement cyclique (voir Delcourt, exercice 1.1.12.).

2. Soit $(G, \cdot)$ un groupe commutatif fini d'ordre $n \geq 2$.

   (a) Montrer que pour tout diviseur premier p de n il existe dans G un élément d'ordre p (lemme de Cauchy dans le cas commutatif). On peut procéder par récurrence sur l'ordre $n \geq 2$ de G en utilisant un groupe quotient $\dfrac{G}{\langle g \rangle}$ où $g \in G \setminus \{1\}$.

   (b) Si d est un diviseur de n non nécessairement premier, existe-il un sous groupe de G d'ordre d.

3. Soit $(G, \cdot)$ un groupe commutatif fini d'ordre $n \geq 2$ et :

$$m = \max_{g \in G} \theta(g) = \text{ppcm}\{\theta(g) \mid g \in G\}$$

   l'exposant de G (question **I.9**).

   (a) En utilisant l'application φ du groupe produit $H = \prod_{g \in G} \langle g \rangle$ dans G définie par :

$$\forall h = (g_1, \cdots, g_n) \in H,\ \varphi(h) = \prod_{i=1}^{n} g_i$$

   montrer que n divise le produit des ordres $\prod_{g \in G} \theta(g)$.

   (b) Montrer que m a les mêmes facteurs premiers que n.

   (c) Déduire de ce qui précède une deuxième démonstration du lemme de Cauchy dans le cas commutatif.

   (d) On désigne par φ la fonction indicatrice d'Euler. Montrer que si $n \geq 2$ est un entier premier avec $\varphi(n)$, alors tout groupe commutatif d'ordre n est cyclique. Réciproquement, on peut montrer que la réciproque est vrai, c'est-à-dire qu'un entier $n \geq 2$ est premier avec $\varphi(n)$, si, et seulement si, tout groupe commutatif d'ordre n est cyclique (voir Francinou et Gianella, exercices de mathématiques pour l'agrégation, Masson).

4. En utilisant la question **I.3** montrer le cas particulier suivant du lemme de Cauchy : si G est un groupe fini d'ordre $2p$ avec p premier, il existe alors un élément d'ordre p dans G.

5. On se propose de montrer le lemme de Cauchy pour tout groupe fini.
   Soit G un groupe fini de cardinal n et p un diviseur premier de n. On note :

$$X = \{(g_1, \cdots, g_p) \in G^p \mid g_1 \cdots g_p = 1\}$$

   (a) Calculer le cardinal de X.

   (b) On désigne par $H = \langle\sigma\rangle$ le sous-groupe de $\mathcal{S}_p$ (groupe des permutations de $\{1, 2, \cdots, p\}$) engendré par le p-cycle $\sigma = (1, 2, \cdots, p)$.
   Montrer que l'application :

$$\left(\sigma^k, (g_1, \cdots, g_p)\right) \mapsto \left(g_{\sigma^k(1)}, \cdots, g_{\sigma^k(p)}\right)$$

   définit une action de H sur X.

   (c) On note X^H l'ensemble des éléments $x \in X$ tels que $H \cdot x = \{x\}$. Montrer que $X^H \neq \emptyset$ et card $\left(X^H\right)$ est divisible par p.

   (d) Déduire de ce qui précède qu'il existe dans G un élément d'ordre p (lemme de Cauchy).

6. Donner une deuxième démonstration du lemme de Cauchy en utilisant le résultat dans le cas commutatif. On peut procéder par récurrence sur l'ordre du groupe et utiliser les résultats de **II.2**.