DM Algèbre Générale
Ordre d'un élément

Exercice 1

Soit p un nombre premier. L'objet de cet exercice est de répertorier les groupes finis à $2p$ éléments. Soit G un tel groupe. On notera la loi multiplicativement et e le neutre de G.

1) Donner les ordres possibles d'un élément de G différent de e.
2) Donner un exemple de groupe cyclique G d'ordre $2p$, en précisant l'ordre de chacun des éléments.
3) Dans cette question, on suppose que G n'est pas cyclique.
   a) Montrer que G possède au moins un sous-groupe cyclique d'ordre p.
   b) Montrer que si $p > 2$, G contient au plus un sous-groupe cyclique d'ordre p.
   c) Décrire alors G.
4) Donner un exemple d'un groupe non cyclique G d'ordre $2p$, en précisant l'ordre de chacun de ses éléments.

Exercice 2

Soit G un groupe fini d'ordre n.

1) On suppose que G est cyclique.
   a) Montrer que tout sous-groupe de G est cyclique.
   b) Montrer que pour tout diviseur d de n dans $\mathbb{N}$, il existe un et un seul sous-groupe de G d'ordre d.
2) Pour tout diviseur d de n, on désigne par $c(d)$ le nombre de sous-groupes cycliques d'ordre d de G et pour tout entier $k \in \mathbb{N}^*$, on désigne par $\varphi(k)$ le nombre d'entiers entre 1 et k, premiers avec k (indicatrice d'Euler de k).
   a) Montrer que si H est un sous-groupe cyclique d'ordre d de G, le nombre de ses éléments générateurs est $\varphi(d)$.
   b) Démontrer alors la relation : $\displaystyle n = \sum_{d|n} c(d)\varphi(d)$.

   (La somme est étendue à tous les diviseurs de n.)
3) En déduire que :
$$\forall n \in \mathbb{N}^*, \quad n = \sum_{d|n} \varphi(d).$$
4) Montrer que si le groupe G possède, pour tout diviseur d de n, au plus un sous-groupe cyclique d'ordre d, alors G est cyclique.

Exercice 3

Soit G un groupe de cardinal n, d'élément neutre e, et p un diviseur premier de n. On veut montrer que G possède au moins un élément d'ordre p (théorème dû à Augustin Cauchy).

On désigne par E l'ensemble des p-uplets d'éléments de G dont le produit est e :

$$E = \{(x_1, \ldots, x_p) \in G^p, \quad x_1 \cdots x_p = e\}.$$

1) Montrer que $\mathrm{Card} E = n^{p-1}$.

2) On considère l'application σ définie sur E définie par : $\sigma(x_1, \ldots, x_p) = (x_2, \ldots, x_p, x_1)$.
   a) Montrer que σ appartient au groupe des bijections de E dans E, et que $\sigma^p = \mathrm{Id}_E$.
   b) Soit $(x_1, \ldots, x_p) \in E$; on désigne par r le plus petit entier strictement positif tel que $\sigma^r(x_1, \ldots, x_p) = (x_1, \ldots, x_p)$. Montrer que $r = 1$ ou p.
   c) Montrer que $r = 1$ si et seulement si $x_1 = \cdots = x_p = x$ où x est un élément de G d'ordre 1 ou p.
   d) Montrer que le nombre d'éléments de E pour lesquels $r = p$ est un multiple de p.

3) On suppose que le groupe G ne possède aucun élément d'ordre p. Trouver une contradiction et conclure.

Corrigé

Exercice 1

1) L'ordre d'un élément de G différent de e est un diviseur supérieur ou égal à 2 du cardinal de G, soit ici $2p$. Donc, les ordres possibles d'un élément de G différent de e sont 2, p et $2p$.

2) L'ensemble G des racines $(2p)$-ièmes complexes de l'unité est un groupe cyclique d'ordre $2p$. Posons pour tout $k \in [\![0, 2p-1]\!]$, $\omega_k = \mathrm{e}^{i\frac{2k\pi}{2p}} = \mathrm{e}^{i\frac{k\pi}{p}}$. Il est clair que pour tout $k \in [\![1, 2p-1]\!]$, $\omega_k^{2p} = 1$ et on a :

$$\begin{cases} \omega_k^2 = 1 \iff \dfrac{2k\pi}{p} \equiv 0 \mod 2\pi \iff p|k, \text{ et comme } k \in [\![1, 2p-1]\!],\ k = p \\ \omega_k^p = 1 \iff \dfrac{pk\pi}{p} = k\pi \equiv 0 \mod 2\pi, \text{ soit } k \text{ est pair.} \end{cases}$$

Ainsi, ω_p est d'ordre 2, ω_k est d'ordre p quand k est pair et d'ordre $2p$ quand k est impair et différent de p.

3) Remarquons que G n'est pas cyclique, donc ne contient aucun élément d'ordre $2p$. Ainsi, tout élément de G différent de e est d'ordre 2 ou p.

a) Si $p = 2$, alors tout élément est d'ordre 2.

Si $p > 2$, supposons que G ne contienne pas de sous-groupe cyclique d'ordre p. Alors, aucun élément n'est d'ordre p, donc tous les éléments de G sont d'ordre 2 (c'est-à-dire leur propre symétrique). Soit alors x_1 et x_2 deux éléments de G distincts et différents de e. On a :

- $x_1x_2 = e \ \Rightarrow\ x_2 = x_1^2x_2 = x_1(x_1x_2) = x_1$, ce qui est absurde, donc $x_1x_2 \neq e$;
- $x_1x_2 = x_1 \ \Rightarrow\ x_2 = e$, ce qui est absurde, donc $x_1x_2 \neq x_2$.

Or, $x_1x_2 = (x_1x_2)^{-1} = x_2^{-1}x_1^{-1} = x_2x_1$, donc x_1 et x_2 commutent.

Alors, $H = \{e, x_1, x_2, x_1x_2\}$ est stable par la loi de G, et comme chaque élément est son propre inverse, H est un sous-groupe de G d'ordre 4. Ceci est absurde car 4 ne divise pas $2p$.

Ainsi, G contient au moins un sous-groupe cyclique d'ordre p.

Remarque : nous avons démontré ici un cas particulier du *théorème de Cauchy* qui énonce que dans tout groupe fini de cardinal n, pour tout diviseur premier p de n, il existe au moins un élément d'ordre p, donc un sous-groupe cyclique d'ordre p. Nous démontrerons ce théorème dans l'exercice 4, plus loin dans ce chapitre.

b) Supposons que G contienne deux sous-groupes cycliques d'ordre p distincts : $H_1 = < x_1 >$ et $H_2 = < x_2 >$.

Comme p est premier, tout élément de H_1 (resp. H_2) différent de e engendre H_1 (resp. H_2). Alors, s'il existe $x \in H_1 \cap H_2$ tel que $x \neq e$, on a $H_1 = H_2 = < x >$, ce qui est absurde. Ainsi, $H_1 \cap H_2 = \{e\}$ et $H_1 \cup H_2$ contient $2p-1$ éléments de G. Soit x_3 le dernier élément de G, autrement dit, celui qui n'appartient ni à H_1, ni à H_2. Cet élément est nécessairement d'ordre 2. Que penser de x_1x_3 et x_3x_1 ? Ces deux éléments sont distincts de x_3 (sinon, on aurait $x_1 = e$) et différents de toute puissance de x_1 (sinon x_3 serait lui-même une puissance de x_1, donc appartiendrait à H_1). Ainsi, ces deux éléments sont dans H_2 et donc $(x_1x_3)(x_3x_1) \in H_2$. Or :

$$(x_1x_3)(x_3x_1) = x_1x_3^2x_1 = x_1^2 \in H_2.$$

Ainsi, $x_1^2 = e$, ce qui est absurde, car $p > 2$ et x_1 est d'ordre p. Finalement, si $p > 2$, G contient au plus un sous-groupe cyclique d'ordre p.

c) D'après ce qui précède, G contient exactement un élément d'ordre p et tous ses autres éléments distincts de e sont d'ordre 2. Donc :

$$G = \left\{e, x_0, x_0^2, \ldots, x_0^{p-1}, x_1, x_2, \ldots, x_p\right\} \text{ avec : } \forall k \in [\![1, p]\!],\ x_k^2 = e.$$

4) Rappelons qu'une isométrie du plan affine euclidien P est une application de P dans P qui conserve les distances. On a les résultats suivants sur les isométries :

• la composée de deux isométries est une isométrie ; toute isométrie est bijective et sa réciproque est une isométrie. Comme l'identité de P est une isométrie, ceci prouve que l'ensemble des isométries de P est un sous-groupe du groupe des bijections de P dans P ;

• les seules isométries du plan ayant au moins un point invariant sont les rotations et les réflexions ;

• l'image d'un polygone régulier convexe par une isométrie est un polygone régulier convexe de même centre, de même nombre de côtés et dont les sommets sont les images des sommets du polygone initial.

Dans le plan P, considérons $A_1A_2\cdots A_p$ un polygone régulier convexe à p côtés, de centre O et appelons G l'ensemble des isométries de P laissant globalement invariant ce polygone.

Alors, l'identité de P est une isométrie qui appartient clairement à G. Si $(f, g) \in G^2$, le polygone $A_1A_2\cdots A_p$ est globalement invariant par g, donc par g^{-1} et par f, donc par $f \circ g^{-1}$. Donc $f \circ g^{-1} \in G$, ce qui prouve que G est un sous-groupe du groupe des isométries de P, donc un groupe.

D'après les propriétés rappelées, pour tout $f \in G$, O est invariant par f, donc f est une rotation ou une réflexion. En passant en revue les images possibles de A_1 par un élément de G et les rotations de centre O ou les réflexions donnant ces images, on prouve assez facilement que :

$$G = \left\{\mathrm{id}, r, r^2, \ldots, r^{p-1}, s_1, s_2, \ldots, s_p\right\},$$

où r est la rotation de centre O et d'angle $\frac{2\pi}{p}$ et s_k est la réflexion ayant pour axe la médiatrice de $[A_kA_{k+1}]$ (en posant $A_{p+1} = A_1$). Toutes les rotations sont d'ordre p (puisque p est premier) et toutes les réflexions sont d'ordre 2. Ainsi, G est bien un groupe non cyclique d'ordre $2p$.

Exercice 2

1) Soit G un groupe cyclique d'ordre n.

a) Soit g un élément générateur de G et H un sous-groupe de G. Considérons l'ensemble $K = \{k \in \mathbb{Z},\ g^k \in H\}$. Il est non vide, puisqu'il contient 0, stable par addition : si $(g^k, g^{k'}) \in H^2$, $g^{k+k'} = g^k g^{k'} \in H$ et il contient les opposés de ses éléments : si $g^k \in H$, $g^{-k} = (g^k)^{-1} \in H$. C'est donc un sous groupe de $(\mathbb{Z}, +)$; il existe $p \in \mathbb{N}$ tel que $K = p\mathbb{Z}$. Notons que $g^n = e \in H$, donc $n \in K$, ce qui prouve que p est un diviseur de n.

Comme $g^p \in H$, le sous-groupe engendré par g^p est inclus dans H : $<g^p> \subset H$. Réciproquement, pour tout $k \in \mathbb{Z}$ tel que $g^k \in H$, $k \in p\mathbb{Z}$: il existe $k' \in \mathbb{Z}$ tel que $k = k'p$, d'où $g^k = g^{k'p} = (g^p)^{k'} \in <g^p>$. Donc $H \subset <g^p>$. En définitive, $H = <g^p>$. H est le groupe cyclique engendré par g^p.

b) Soit d un diviseur de n ; posons $n = dp$ et considérons le sous-groupe $H = <g^p>$, d'ordre h. On a $(g^p)^d = g^n = e$; comme g^p est d'ordre h, $h|d$. De plus, $g^{ph} = (g^p)^h = e$; comme g est d'ordre n, $n|ph$, d'où $d|h$. En définitive, $h = d$. Le sous-groupe H est d'ordre d. On a nécessairement $p = \frac{n}{d}$, ce qui implique que H est le seul sous-groupe de G d'ordre d.

2) a) Soit d un diviseur de n et $<x>$ un éventuel sous-groupe cyclique d'ordre d de G. L'application θ de $\mathbb{Z}/d\mathbb{Z}$ dans $<x>$: $\dot{k} \mapsto x^k$ (bien définie, puisque si $k \equiv k'\,[d]$, $x^k = x^{k'}$) est un morphisme de groupes. Comme $x^k = e$ équivaut à $k \in d\mathbb{Z}$, c'est-à-dire à $\dot{k}=\dot{0}$ modulo d, le noyau de θ est $\{\dot{0}\}$, donc θ est injectif.
Or, $\mathrm{Card}\big(\mathbb{Z}/d\mathbb{Z}\big) = \mathrm{Card}\big(<x>\big) = d$, donc θ est bijectif : c'est un isomorphisme.

On sait que les éléments générateurs de $\mathbb{Z}/d\mathbb{Z}$ sont les classes $\dot{k}$, où k est premier avec d. Il y en a donc $\varphi(d)$. Les éléments générateurs de $<x>$ sont les images par θ de ceux de $\mathbb{Z}/d\mathbb{Z}$. Ces images sont distinctes deux à deux, il y en a donc également $\varphi(d)$.

b) Tout élément de G est générateur d'un sous-groupe cyclique d'ordre d, où d est un diviseur de n. Chacun de ces $c(d)$ sous-groupes possède $\varphi(d)$ éléments générateurs. D'où :

$$n = \sum_{d|n} c(d)\varphi(d).$$

3) En particulier, en appliquant la relation précédente à un groupe cyclique, on a, pour tout diviseur d de n, $c(d) = 1$ d'après la question 1)b, et donc :

$$\forall n \in \mathbb{N}^*, \quad n = \sum_{d|n} \varphi(d).$$

4) Si pour le groupe G, on suppose que, pour tout d divisant n, $c(d) \leqslant 1$, on a :

$$n = \sum_{d|n} c(d)\varphi(d) \leqslant \sum_{d|n} \varphi(d) = n.$$

Cette relation n'est possible que si pour tout d, $c(d) = 1$. En particulier, $c(n) = 1$: le groupe G tout entier est cyclique.

Exercice3

1) Un élément de E est entièrement déterminé par les $p-1$ éléments $x_1, \ldots, x_{p-1}$ que l'on peut choisir librement ; le dernier sera donné par $x_p = x_{p-1}^{-1} \ldots x_1^{-1}$. On en déduit : $\mathrm{Card}E = n^{p-1}$.

2) On considère l'application σ de E dans E définie par : $\sigma(x_1, \ldots, x_p) = (x_2, \ldots, x_p, x_1)$.

a) Si $(x_1, x_2, \ldots, x_p) \in E$, $x_1 x_2 \cdots x_p = e$, donc $x_2 \cdots x_p = x_1^{-1}$ et $x_2 \cdots x_p x_1 = e$, ce qui signifie que $(x_2, \ldots, x_p, x_1) = \sigma(x_1, x_2, \ldots, x_p) \in E$: σ est une application de E dans E. Tout élément $(x_1, \ldots, x_p)$ de E possède un antécédent unique par σ, qui est $(x_p, x_1, \ldots, x_{p-1})$; donc σ est une bijection. En répétant σ p fois, on revient au point de départ : $\sigma^p = \mathrm{Id}_E$.

b) Soit $(x_1, \ldots, x_p) \in E$; l'ensemble H des entiers k tels que $\sigma^k(x_1, \ldots, x_p) = (x_1, \ldots, x_p)$ est un sous-groupe de $\mathbb{Z}$. Comme r est le plus petit élément strictement positif de H, on a $H = r\mathbb{Z}$. Comme $\sigma^p = \mathrm{Id}_E$, $p \in H$, donc p est un multiple de r, et comme il est premier, $r = 1$ ou p.

c) $r = 1$ si et seulement si $(x_1, \ldots, x_p)$ est invariant par σ, c'est-à-dire si $x_1 = \cdots = x_p$. On a alors $(x, x, \ldots, x) \in E$, c'est-à-dire $x^p = e$: l'ordre de x divise p. Comme p est premier, cet ordre est 1 ou p.

d) Si $r = p$, les p éléments $(x_1, \ldots, x_p)$, $(x_2, \ldots, x_p, x_1)$, … $(x_p, x_1, \ldots, x_{p-1})$ sont tous distincts et vérifient tous $r = p$. L'ensemble des éléments $(x_1, \ldots, x_p)$ tels que $r = p$ peut donc être partitionné en sous-ensembles de cardinal p. On en déduit que le nombre de tels éléments est multiple de p.

3) Supposons que le groupe G ne possède aucun élément d'ordre p. Il n'existe alors qu'un seul élément dans E vérifiant $r = 1$: c'est $(e, e, \ldots, e)$. On a donc : $n^{p-1} = 1 + N$ où N est le nombre d'éléments de E vérifiant $r = p$. Or n^{p-1} et N sont tous deux des multiples de p. On aboutit à une contradiction, qui nous permet de conclure :

Théorème de Cauchy : dans tout groupe de cardinal n, pour tout nombre premier p qui divise n, il existe au moins un élément d'ordre p.