Université Paris 7 **Deuxième semestre 2003-2004**
DEUG MIAS Info - 1ère année **MT132 - groupe 1B4**

Complément

Groupes cycliques

Rappel : Soit G un groupe fini de neutre 1. Si a est un élément de G, $< a >$ désigne le *sous-groupe de G engendré par a*. C'est l'ensemble $\{a^m \mid m \in \mathbb{Z}\}$. Si n désigne l'ordre de a, alors ce sous-groupe est $< a >= \{1, a, a^2, \ldots, a^{n-1}\}$ (remarquer que $< a >$ est d'ordre n).
Cas particulier : si $a = 1$ alors $< a >= \{1\}$.

De façon générale, $< a >$ est un sous-ensemble de G, pas forcément égal à G.

Définition. Un groupe fini G est *cyclique* s'il existe un élément $a \in G$ tels que $< a >= G$. Cela signifie qu'il existe un élément a de G qui engendre G tout entier. Un tel élément a est appelé un *générateur* de G.

Exemple 0. Soit G un groupe fini et a un élément de G. Regardons le sous-groupe $< a >$ de G comme un groupe. Alors c'est un groupe cyclique car il est engendré par l'élément a.

Exemple 1. (Feuille 6, exercice 10). Soit $H = \{id, (1234), (13)(24), (1432)\}$. Alors H est un groupe cyclique. En effet, si on note $\sigma = (1234)$, alors un calcul montre que $\sigma^2 = (13)(24)$, $\sigma^3 = (1432)$ et $\sigma^4 = id$. Donc σ est d'ordre 4 et $H = \{id, \sigma, \sigma^2, \sigma^3\} =< \sigma >$.

Contre-exemple. (Feuille 6, exercice 10). Soit $G = \{id, (12)(34), (13)(24), (14)(23)\}$. Ce n'est pas un groupe cyclique. En effet :

- id est d'ordre 1 donc $< id >= \{id\} \subsetneq G$
- $(12)(34)$ est d'ordre 2 (c'est un produit de 2-cycles de supports disjoints), donc $< (12)(34) >$ est formé de deux éléments. On a $< (12)(34) > \subsetneq G$.
- idem pour $(13)(24)$ et $(14)(23)$.

Exemple 2. (Feuille 6, exercice 3). Soit n un entier ≥ 1. Le groupe multiplicatif $\mathbb{U}_n$ des racines $n$èmes de l'unité est formé de $1, e^{\frac{2i\pi}{n}}, e^{\frac{2.2i\pi}{n}}, \ldots, e^{\frac{(n-1)2i\pi}{n}}$. Démontrons que c'est un groupe cyclique. Posons $z = e^{\frac{2i\pi}{n}}$. Alors z est d'ordre n car $z, z^2, \ldots, z^{n-1}$ sont distincts de 1 et $z^n = 1$. De plus, on remarque que $1 = z^0, e^{\frac{2i\pi}{n}} = z, e^{\frac{2.2i\pi}{n}} = z^2, \ldots, e^{\frac{(n-1).2i\pi}{n}} = z^{n-1}$. Donc $\mathbb{U}_n = \{1, z, z^2, \ldots, z^{n-1}\}$. Comme z est d'ordre n, $< z >= \{1, z, z^2, \ldots, z^{n-1}\}$. Donc $\mathbb{U}_n =< z >$. Ceci montre que $\mathbb{U}_n$ est cyclique et engendré par z.
En particulier, z est un générateur de $\mathbb{U}_n$. L'objet de la question 2 de l'exercice est de déterminer tous les générateurs de $\mathbb{U}_n$.

Exemple 3. (Feuille 6, exercice 4). Soit G un groupe de cardinal p premier. Démontrons que G est cyclique et engendré par n'importe quel élément de G distinct du neutre.
Soit $x \in G$, $x \neq e$. Alors $< x >$ est un sous-groupe de G. D'après le théorème de Lagrange, $\text{Card}(< x >)$ divise $\text{Card}(G) = p$. Comme p est premier, $\text{Card}(< x >)$ vaut 1 ou p.

Supposons Card($< x >$) = 1. Comme $e \in < x >$, on a $< x >= \{e\}$, donc $x = e$ ce qui est exclu.
Donc Card($< x >$) = p. Finalement, on a une inclusion $< x > \subset G$ et une égalité des cardinaux, donc $< x >= G$. C'est le résultat souhaité.

Résultat. Soit G un groupe fini d'ordre n. Alors G est cyclique si et seulement s'il existe un élément a de G d'ordre n.

Preuve. Supposons G cyclique. Alors il existe $a \in G$ tel que $G =< a >$. Donc $< a >$ est d'ordre n. Donc l'élément a est d'ordre n. Réciproquement, supposons qu'il existe a dans G d'ordre n. Alors $< a >$ est un sous-groupe de G d'ordre n, donc par égalité de cardinal, $< a >= G$. Ceci montre que G est cyclique.

Résultat. Tout sous-groupe d'un groupe cyclique est cyclique.

Exemple 4. (Feuille 6 exercice 5). Si G et H sont deux groupes cycliques, alors le groupe produit $G \times H$ est cyclique.