Résumé de cours : *Groupes cycliques. Groupes symétriques.*

MPSI-Maths.
Mr Mamouni : *myismail@altern.org*

1 Groupes cycliques.

Ordre d'un groupe.

Définition 1. *Si G est un groupe, son cardinal est appellé alors l'ordre de G et noté $o(G)$.*

Vocabulaire.

Tout groupe fini est dit d'ordre fini.

Groupe engendré par un élément.

Définition 2. *Soit $(G,.)$ un groupe et $a \in G$, on appelle sous groupe engendré par a le sous-groupe de G, noté $< a >$ formé par les puissances de a.*
Autrement dit : $< a >= \{a^n \text{ tel que : } n \in \mathbb{Z}\}$.

Remarque.

Soit $(G,.)$ un groupe et $a \in G$, alors $< a >$ est le plus petit sous-groupe de G contenant a.

Autrement dit : Si H est un sous-groupe de G, $a \in H \Longrightarrow < a > \subset H$.

Ordre d'un élément d'un groupe.

Définition 3. *Soit $(G,.)$ un groupe et $a \in G$. L'ordre du sous-groupe engendré par a est aussi appelé l'ordre de a, et noté $o(a)$.*
Autrement dit : $o(< a >) = o(a)$.

Remarque.

Soit $(G,.)$ un groupe et $a \in G$, alors $o(a) = 1 \Longleftrightarrow a = e$, où e l'élément neutre de G.

Vocabulaire.

Un élément d'un groupe est dit d'ordre fini, lorsqu'il engendre un groupe fini.

Théoréme 1. *Soit $(G,.)$ un groupe et $a \in G$, alors :*
a est d'ordre fini $\Longleftrightarrow \exists n \in \mathbb{N}^*$ tel que : $a^n = e$.

Théoréme 2. *Soit $(G,.)$ un groupe et $a \in G$, alors :*
a est d'ordre fini $\Longleftrightarrow \exists n \in \mathbb{N}^*$ tel que : $a^n = e$.

Théoréme 3. *Soit $(G,.)$ un groupe et $a \in G, n \in \mathbb{N}$, alors :*

$$o(a) = n \Longleftrightarrow \begin{cases} i) & a^n = e \\ ii) & \forall k \in \mathbb{N}, \quad a^k = e \Longrightarrow n \text{ divise } k \end{cases}.$$

Groupes monogènes.

Définition 4. *Un groupe G est dit monogène s'il est engendré par l'un de ses éléments.*
Autrement dit : $\exists a \in G$ tel que : $G =< a >$.

Définition 5. *Un groupe G est dit cyclique s'il est monogène et fini.*

2 Groupes symétriques.

Permutaion :

Définition 6. *On appelle permutation de* $[|1,n|]$ *toute bijection :* $\sigma : [|1,n|] \to [|1,n|]$. *L'ensemble de ces permutaions se note* $\mathcal{S}_n$*, muni de la loi o est un groupe non abélien de cardinal* $n!$*, appellé groupe symétrique d'ordre* n.

Support :

Définition 7. *Soit* $\sigma \in \mathcal{S}_n$*, on appelle support de* σ*, l'ensemble* $supp(\sigma) = \{k \in [|1,n|]$ *tel que :* $\sigma(k) \neq k\}$.

Transposition :

Définition 8. *On appelle transposition toute permutation dont le support est formé par deux éléments. Dans ce cas si* $supp(\sigma) = \{i,j\}$ *alors* $\sigma(i) = j, \sigma(j) = i$*, on note alors* $\sigma = (i \quad j)$ *et on a :* $\sigma^2 = id_{[|1,n|]}$.

p-cycles :

Définition 9. *On dit que* σ *est un p-cycle si* $\exists (i_1, i_2, \ldots, i_p) \in [|1,n|]^p$ *tel que :* $supp(\sigma) = \{i_1, i_2, \ldots, i_p\}$ *avec* $\sigma(i_k) = i_{k+1} \quad \forall 1 \leq k \leq p-1$ *et* $\sigma(i_p) = i_1$.

Notation :

Dans ce cas on écrit $\sigma = (i_1 \quad i_2, \ldots i_p)$ et on a : $\sigma^p = id_{[|1,n|]}$.

Remarque.

- Notez bien que les transpostions sont des 2-cycles.
- $(i_1 \quad i_2, \ldots i_p) = (i_1 \quad i_2)(i_2 \quad i_3)\ldots(i_{p-1} \quad i_p)$. C'est à dire que tout p-cycle peut s'écrire comme produit de $p-1$ transposions.

Théoréme 4. *Toute permutation peut s'écrire comme produit de p-cycles. On dit que* $\mathcal{S}_n$ *est engendré par les p-cycles.*

Corollaire 1. *Toute permutation peut s'écrire comme produit de transposition. On dit que* $\mathcal{S}_n$ *est engendré par les transpositions.*

Inversion :

Définition 10. *On appelle inversion de* σ*, tout couple* $(i,j) \in [|1,n|]^2$ *tel que :* $i < j$ *et* $\sigma(i) > \sigma(j)$.

Signature :

Définition 11. *On appelle signature de* σ*, noté* $\varepsilon(\sigma) = \pm 1$*, définie par* $\varepsilon(\sigma) = (-1)^{\text{Nombre d'inversions de } \sigma}$.

Remarque.

La signature définit un morphisme de group entre $(\mathcal{S}_n, o)$ et $(\{-1,1\} \times)$, c'est à dire que $\forall (\sigma, \tau) \in \mathcal{S}_n^2$ on a : $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.

Théoréme 5. *la signature d'une transposition est toujours -1.*

Théoréme 6. *la signature d'un p-cycle est toujours* $(-1)^p$.

Théoréme 7. *On appelle permutation paire toute permutation de signature 1.*

Groupe alterné :

Définition 12. *L'ensemble des pemutations paires se note* $\mathcal{A}_n$*, c'est un sous-groupe de* $\mathcal{S}_n$*, de cardinal* $\frac{n!}{2}$*, on l'appelle groupe alterné d'ordre* n.

Théoréme 8. *Toute permutation paire peut s'écrire comme produit de 3-cycles. On dit que* $\mathcal{A}_n$ *est engendré par les 3-cycles.*

Fin.