21 – Compléments sur les groupes finis

Cours TD

1 Théorème de Lagrange

1.1 Ordre d'un élément

Proposition 1.1 (*)
Soit G un groupe fini, soit $x \in G$. Il existe $n \in \mathbb{N}^*$ tel que $x^n = e_G$.

Indication
Considérer deux indices $i \neq j$ tels que $x^i = x^j$.

Définition 1.2
Le plus petit entier n dans la proposition précédente est l'ordre de x. On le note $\omega_G(x)$.

Proposition 1.3 (*)
Pour tout $n \in \mathbb{Z}$, $x^n = e_G \iff \omega_G(x) \mid n$.

Indication
Faire une division euclidienne.

Théorème 1.4 (** – Lagrange – cas abélien)
Si G est abélien, $\omega_G(x)$ divise $|G|$.

Indication
Considérer le produit $P = \prod_{y \in G} y$.

Remarque 1.5
Le théorème est encore vrai si G n'est pas abélien. Cependant, la démonstration est HP.

Exemples 1.6
- Soit p un nombre premier. Soit $x \in \mathbb{Z}$ premier avec p. Alors $x^{p-1} \equiv 1\,[p]$ (petit théorème de Fermat).
  Notons en effet u la classe de x modulo p. C'est un élément de $\left(\mathbb{Z}/p\mathbb{Z}\right) \setminus \{0\}$, groupe abélien (multiplicatif) de cardinal $p-1$. Donc, u^{p-1} est la classe de 1 modulo p, ce qui revient à dire que $x^{p-1} \equiv 1\,[p]$.

– Si le cardinal d'un groupe G est un nombre premier p, alors G est cyclique. En effet, si $x \neq \{e_G\}$ est un élément de G, son ordre doit diviser p. Comme il est différent de 1, il est égal à p. Ceci montre que x est un générateur de G, donc que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (cf. section suivante).

1.2 Théorème de Lagrange – cas général

Lemme 1.7 (**)
Soit G un groupe fini, soit H un sous-groupe de G. On définit une relation d'équivalence $\mathcal{R}_H$ par : $\forall x, y \in G, x \mathcal{R}_H y \iff xy^{-1} \in H$.
Toutes les classes d'équivalence ont même cardinal $|H|$.

Indication
Décrire simplement les classes d'équivalence pour les mettre en bijection avec H.

Corollaire 1.8 (* – HP)
Si G est un groupe fini et H un sous-groupe, alors $|H|$ divise $|G|$.

Corollaire 1.9 (* – Lagrange – cas général)
Si G est un groupe fini et si $x \in G$, $\omega_G(x)$ divise $|G|$.

Indication
Considérer le sous-groupe $\langle x \rangle$ engendré par x. Montrer que son cardinal est $\omega_G(x)$.

Remarque 1.10
On peut réciproquement se demander si, dans un groupe G de cardinal n, on peut trouver un élément d'ordre un diviseur d de n fixé.
C'est faux en général puisque l'existence d'un élément d'ordre n lui-même est équivalente au caractère cyclique de G. Cependant, si p est un nombre premier divisant n, alors il existe un élément d'ordre p (lemme de Cauchy) ; on peut même raffiner : si p^α divise n, alors il existe un sous-groupe de G de cardinal p^α.

2 Groupes cycliques

2.1 Description des groupes cycliques

Définition 2.1
Un groupe cyclique est un groupe fini engendré par un élément.

Théorème 2.2 (**)
Si G est un groupe cyclique de cardinal n, alors G est isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Indication
Si x est un générateur de G, considérer $\phi : \mathbb{Z}/n\mathbb{Z} \to G, \bar{k} \mapsto x^k$.

Exemple 2.3
Le groupe multiplicatif $\mathbb{U}_n$ des racines n-èmes de l'unité est engendré par $e^{2i\pi/n}$. Il est donc isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$.
En pratique, $\mathbb{U}_n$ peut servir de *modèle* aux groupes cycliques autant que $\mathbb{Z}/n\mathbb{Z}$: ou bien les calculs sont écrits multiplicativement avec une exponentielle complexe ; ou bien les calculs sont écrits additivement avec des classes d'entiers modulo n.

Proposition 2.4 (**)
Si G est un groupe cyclique de cardinal n, tous les sous-groupes de G sont cycliques et, si d est un diviseur de n, il existe exactement un sous-groupe de G de cardinal d.

Indication
Il est plus aisé de travailler avec $\mathbb{U}_n$.

Remarque 2.5
Un produit de groupes cycliques n'est pas cyclique en général. En fait, le théorème de structure des groupes abéliens finis affirme que tout groupe abélien fini est isomorphe à un produit de groupes cycliques.

Proposition 2.6 (**)
Si G et H sont deux groupes cycliques de cardinal n et m premiers entre eux, alors $G \times H$ est cyclique.

Indication
Construire un générateur de $G \times H$ à partir de générateurs de G et H.

Remarque 2.7
Une version plus précise du théorème dit qu'on a un isomorphisme d'anneaux

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

si n et m sont premiers entre eux.

2.2 Indicatrice d'Euler

Définition 2.8
Soit $n \in \mathbb{N}^*$. L'indicatrice d'Euler $\phi(n)$ est le nombre d'entiers $k \in [\![1, n]\!]$ premiers avec n.

Proposition 2.9 (***)
On a les propriétés suivantes :
- $\phi(n)$ *est le cardinal du groupe des inversibles de l'anneau* $\mathbb{Z}/n\mathbb{Z}$.
- $\phi(n)$ *est le nombre de générateurs du groupe additif* $\mathbb{Z}/n\mathbb{Z}$.
- *Pour tout* $a \in \mathbb{Z}$ *premier avec* n, $a^{\phi(n)} \equiv 1\,[n]$.
- $\sum_{d|n} \phi(d) = n$.

Indication
Pour le dernier point, compter le nombre d'éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$. On utilisera la Proposition 2.4 et le deuxième point.

Théorème 2.10 (***)
Si K *est un corps fini, le groupe multiplicatif* K^* *est cyclique.*

Indication
Montrer que pour tout diviseur d de n, il y a 0 ou $\phi(d)$ éléments d'ordre d dans K^*. Puis, utiliser la proposition précédente.

Remarque 2.11
Même pour les corps finis $\mathbb{F}_p$, il n'y a pas de formule générale pour déterminer un générateur du groupe des inversibles. Il y en a $\phi(p-1)$ et donc la probabilité qu'une classe modulo p (non nulle) prise au hasard soit un générateur est $\dfrac{\phi(p-1)}{p-1}$.
Par exemple, $\phi(12) = 4$ et il y a donc 4 générateurs pour les inversibles de $\mathbb{F}_{13}$. On constate que $2^6 = 64 \equiv -1\,[13]$, donc la classe de 2 est d'ordre 12 dans les inversibles de $\mathbb{F}_{13}$: c'en est un générateur.

Exercice 2.12
Écrire un programme Python calculant un (les) générateur(s) de $\mathbb{F}_p$.

3 Groupe symétrique

3.1 Décomposition en produit de cycles à supports disjoints

Définition 3.1 (Groupe symétrique)
Soit $n \in \mathbb{N}^*$. On note $\mathcal{S}_n$ le groupe des permutations de $[\![1, n]\!]$.

Notation 3.2 (Écriture d'une permutation)
Pour écrire une permutation $\sigma \in \mathcal{S}_n$, on utilise une notation matricielle. Sur la première ligne, on énumère les entiers de 1 à n ; sur la deuxième ligne, on écrit leur image par σ.

Exemple 3.3
Pour $n = 4$, la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ est la permutation telle que $\sigma(1) = 4$, $\sigma(2) = 2$, $\sigma(3) = 1$ et $\sigma(4) = 1$.

Définition 3.4 (Orbite d'un point)
Soit $\sigma \in S_n$, soit $k \in [\![1, n]\!]$. L'orbite de k sous σ est l'ensemble $\left\{\sigma^\ell(k), \ell \in \mathbb{Z}\right\}$.

Remarque 3.5
Si ω est l'ordre de σ, on a $\sigma^{\omega-1} = \sigma^{-1}$. Plus généralement, $\sigma^{-\ell} = \sigma^{\ell(\omega-1)}$, pour tout $\ell \in \mathbb{N}$. Donc, dans la définition précédente, on peut se limiter aux puissances positives de σ.

Exemples 3.6
- Pour la permutation σ définie plus haut, l'orbite de 1 est l'ensemble $\{1, 4, 3\}$. L'orbite de 2 est l'ensemble $\{2\}$.
- Si σ est l'identité de $[\![1, n]\!]$, l'orbite de k sous σ est réduite au singleton $\{k\}$.

Proposition 3.7 (* – Les orbites forment une partition de $[\![1, n]\!]$)
Soit $\sigma \in \mathcal{S}_n$. L'ensemble des orbites sous σ définit une partition de $[\![1, n]\!]$.

Définition 3.8 (Cycle, support)
Soit $p \geq 2$ un entier. Un p-cycle de $\mathcal{S}_n$ est une permutation σ de $\mathcal{S}_n$ pour laquelle il existe p éléments $a_1, \ldots, a_p$ dans $[\![1, n]\!]$, deux à deux distincts, tels que
- $\forall x \notin \{a_1, \ldots, a_p\}, \sigma(x) = x$
- $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, $\ldots$, $\sigma(a_{p-1}) = a_p$ et $\sigma(a_p) = a_1$.

Le support du p-cycle est l'ensemble $\{a_1, \ldots, a_p\}$, c'est-à-dire l'ensemble des x dans $[\![1, n]\!]$ tels que $\sigma(x) \neq x$.

Définition 3.9 (Transposition)
On appelle transposition un 2-cycle.

Notation 3.10 (Écriture des cycles)
Avec les notations de la définition ci-dessus, le cycle se note $\begin{pmatrix} a_1 & a_2 & \ldots & a_p \end{pmatrix}$.

Exemple 3.11
On reprend l'exemple de la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$. C'est un 3-cycle, qui s'écrit simplement $\begin{pmatrix} 1 & 4 & 3 \end{pmatrix}$. On notera que l'écriture allégée d'un p-cycle n'est pas unique. Ici,

$$\begin{pmatrix} 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 4 \end{pmatrix}.$$

Attention !
Une permutation n'est pas caractérisée par sa partition en orbites. Pour $n = 4$, les 3-cycles $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ et $\begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$ ont toutes les deux comme orbites $\{1, 2, 3\}$ et $\{4\}$.

Théorème 3.12 (** – Décomposition en produit de cycles à supports disjoints)
Soit $\sigma \in \mathcal{S}_n$. Il existe un entier $k \geq 0$, des entiers $p_1, \ldots, p_k \geq 2$, des permutations $\sigma_1, \ldots, \sigma_k$ telles que :
- *Pour tout $i \in [\![1, k]\!]$, σ_i est un p_i-cycle.*
- *Les supports des σ_i sont deux à deux disjoints.*
- *$\sigma = \sigma_1 \circ \cdots \circ \sigma_k$.*

Une telle décomposition de σ est unique à l'ordre près*, au sens où l'ensemble $\{\sigma_1, \ldots, \sigma_k\}$ est entièrement déterminé par σ et par les conditions ci-dessus.*

Indication
Le faire à la main sur des exemples pour comprendre l'algorithme.

Remarque 3.13
Comme les supports des cycles σ_i sont disjoints, ces cycles commutent deux à deux.

Méthode 3.14 (Écriture en produit de cycles)
Pour écrire une permutation sous cette forme, on suit l'algorithme suivant :
- On commence par l'élément 1 et on écrit les éléments $\sigma^k(1)$ dans l'ordre d'apparition ($k \geq 1$) jusqu'à boucler sur 1 (si 1 est envoyé sur lui-même, il n'apparait pas dans la décomposition).
- On a alors traité l'orbite de 1. On prend le premier entier qui n'est pas dans l'orbite de 1 et on recommence.
- On procède ainsi jusqu'à avoir épuisé tous les éléments de $[\![1, n]\!]$.

Par exemple, pour $n = 8$, on considère $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 7 & 1 & 3 & 5 & 8 & 6 \end{pmatrix}$. On calcule

$$\sigma = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 7 & 8 & 6 & 5 \end{pmatrix}.$$

Remarque 3.15
Le *produit* des permutations étant en réalité une composition, le calcul d'un produit de cycles se fait de droite à gauche.

Exemple 3.16
On souhaite écrire comme produit de cycles à supports disjoints la permutation

$$\sigma = \begin{pmatrix} 1 & 3 & 7 \end{pmatrix} \begin{pmatrix} 3 & 2 & 5 & 6 \end{pmatrix} \begin{pmatrix} 5 & 4 & 1 \end{pmatrix}.$$

- 1 est envoyé sur 6, 6 sur 7, 7 sur 1.
- 2 est envoyé sur 5, 5 sur 4, 4 sur 3, 3 sur 2.

Donc, $\sigma = \begin{pmatrix} 1 & 6 & 7 \end{pmatrix} \begin{pmatrix} 2 & 5 & 4 & 3 \end{pmatrix}$.

Théorème 3.17 (** – Les transpositions engendrent $\mathcal{S}_n$)
Toute permutation σ de $\mathcal{S}_n$ s'écrit comme un produit de transpositions.

Indication
Penser au tri par bulles.

Remarque 3.18
Il n'y a pas unicité. Par exemple, le 3-cycle $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$ est égal à $\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}$, mais aussi à $\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix}$.

3.2 Inversions et signature

Définition 3.19 (Inversion d'une permutation)
Soit σ un élément de $\mathcal{S}_n$. Une *inversion* de σ est un couple (k, ℓ) d'entiers de $[\![1, n]\!]$, tels que $k < \ell$ et $\sigma(k) > \sigma(\ell)$.

Notation 3.20 (Nombre d'inversions)
On note $I(\sigma)$ le nombre d'inversions de σ.

Définition 3.21 (Signature d'une permutation)
La signature de σ – notée $\varepsilon(\sigma)$ – est le nombre $(-1)^{I(\sigma)}$.

Exercice 3.22 (**)
Montrer que la signature d'une transposition est égale à -1.

Indication
Tout compter soigneusement.

Lemme 3.23 (**)
Pour tout $\sigma \in \mathcal{S}_n$, $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$.

Indication
Séparer le produit et faire proprement un changement de variables.

Théorème 3.24 (** – La signature est un morphisme de groupes)
Le morphisme de signature $\varepsilon : \mathcal{S}_n \to \{\pm 1\}$ *est un morphisme de groupes :*

$$\forall \sigma, \tau \in \mathcal{S}_n, \varepsilon(\sigma \circ \tau) = \varepsilon(\sigma)\varepsilon(\tau).$$

Indication
Utiliser la formule précédente.

Corollaire 3.25 (* – Signature d'un p-cycle)
La signature d'un p*-cycle est* $(-1)^{p-1}$.

Corollaire 3.26 (* – Signature d'une permutation écrite en produit de cycles)
On suppose que, dans la décomposition en produits de cycles à supports disjoints de σ, il y a k cycles de longueur $p_1, \ldots, p_k$. La signature de σ est $(-1)^{\sum_{i=1}^{k} p_i - k}$.

4 Exemples de groupes finis

Proposition 4.1 (*)
Un groupe de cardinal p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Proposition 4.2 (**)
À isomorphisme près, il existe deux groupes de cardinal 4 : $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Indication
Si G n'a pas d'élément d'ordre 4, montrer que tous les éléments non triviaux sont d'ordre 2 et que G est abélien. Conclure en décrivant les éléments et en écrivant la table de multiplication de G.

Proposition 4.3 (***)
À isomorphisme près, il existe deux groupes de cardinal 6 : $\mathbb{Z}/6\mathbb{Z}$ et $\mathcal{S}_3$.

Indication
Si G n'a pas d'élément d'ordre 6, montrer qu'il a un élément d'ordre 2 et un élément d'ordre 3 et qu'ils ne commutent pas. Décrire tous les éléments et la table de multiplication du groupe et reconnaître celle de $\mathcal{S}_3$.

Proposition 4.4 (****)
À isomorphisme près, il existe 5 groupes de cardinal 8 : $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$ et deux groupes non abéliens : le groupe diédral D_8 et le groupe des quaternions H_8.

Remarque 4.5
On se contente de décrire les deux groupes non abéliens.

- Le groupe diédral D_8 peut être défini comme le groupe des isométries du plan préservant les sommets d'un carré. Il est isomorphe au sous-groupe de $\mathcal{S}_4$ engendré par $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 3 \end{pmatrix}$.
- On peut écrire les éléments de H_8 comme ± 1, $\pm i$, $\pm j$, $\pm k$, qui vérifient entre autres relations $i^2 = j^2 = k^2 = -1$ et $ij = k$. On peut le réaliser comme le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par les matrices I et J définies par

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ et } J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$