Développements :

- Cyclicité de $(\mathbb{Z}/n\mathbb{Z})^\times$
- Simplicité du groupe alterné

Références :

- Algèbre - Tome 2 - Groupes, Szpirglas
- Cours d'algèbre, Perrin
- Mathématiques pour l'agrégation, Rombaldi
- Théorie des groupes, Ulmer

1. Généralités

On fixe un groupe fini G, dont l'élément neutre sera toujours noté 1.

1.1. Ordre d'un élément [Ulmer]

- Def : l'ordre de $g \in G$ est l'ordre du groupe cyclique engendré par g
- Ex : i est d'ordre 4 dans $\mu_8(\mathbb{C})$
- Prop : l'ordre de $g \in G$ est le plus petit $n \in \mathbb{N}^*$ tel que $g^n = 1$

1.2. Groupes quotients [Szpirglas, Ulmer]

- Def : l'indice de $H \trianglelefteq G$ est l'ordre du groupe G/H
- Thm : $|G| = |H|\,[G : H]$
- Thm (Lagrange) : si $H \leq G$, alors $|H|$ divise $|G|$
- Cor : si $g \in G$, alors l'ordre de g divise $|G|$
- App : si $a, b \in G$ commutent et sont respectivement d'ordres m, n premiers entre eux, alors ab est d'ordre mn

1.3. Actions de groupes

On fixe un ensemble fini X.

1.3.1. Cadre théorique général [Szpirglas]

- Def : action de groupe (à gauche/droite) $G \curvearrowright X$
- Ex : action $\mathfrak{S}_n \curvearrowright \{1, \dots, n\}$
- Rmq : cela revient à se donner un morphisme $G \to \mathfrak{S}(X)$
- Def : orbites de X sous l'action de G

- Notation : l'orbite d'un élément $x \in X$ sera notée $\mathrm{Orb}_G(x)$
- Def : stabilisateur d'un élément $\mathrm{Stab}_G(x)$
- Prop : les orbites de X sous l'action de G forment une partition de X, et l'application $G/\mathrm{Stab}_G(x) \to \mathrm{Orb}_G(x)$ définie par $\overline{g} \longmapsto g \cdot x$ est une bijection
- Cor : $|\mathrm{Orb}_G(x)|$ divise $|G|$ et $|G| = |\mathrm{Orb}_G(x)|\,|\mathrm{Stab}_G(x)|$
- Prop : si $x, y \in X$ sont dans la même orbite, alors $\mathrm{Stab}_G(x)$ et $\mathrm{Stab}_G(y)$ sont conjugués (plus précisément, $\mathrm{Stab}_G(g \cdot x) = g\,\mathrm{Stab}_G(x)g^{-1}$)
- Thm : équation aux classes

1.3.2. Application aux p-groupes [Szpirglas]

- Def : p-groupe
- Prop : si G est un p-groupe, alors $|Z(G)| \geq p$
- Cor : si G est d'ordre p^2, alors G est abélien
- Notation : $X^G = \{x \in X \mid \mathrm{Stab}_G(x) = G\}$
- Prop : si G est un p-groupe, alors $|X| \equiv \left|X^G\right| \bmod p$
- Thm : Cauchy

1.3.3. Formule de Burnside [Caldero-Peronnier, Szpirglas]

- Def : fixateur $\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}$
- Rmq : $X^G = \bigcap_{g \in G} \mathrm{Fix}(g)$
- Formule de Burnside
- App : la probabilité que deux éléments de G commutent vaut c/n où c est le nombre de classes de conjugaison dans G
- App : moyenne et variance du nombre de points fixes d'une permutation aléatoire

2. Groupes cycliques

2.1. Définitions et résultats généraux [Rombaldi, Ulmer]

- Def : groupe cyclique
- Ex : $(\mathbb{Z}/n\mathbb{Z}, +)$, $(\mu_n(\mathbb{C}), \times)$
- Contre-ex : $(\mathbb{Z}/p\mathbb{Z})^2$ n'est pas cyclique pour p premier
- Prop : si G est cyclique, alors G est abélien
- Prop : si G est cyclique d'ordre n, alors $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$
- Thm : si $G = \langle g \rangle$ est cyclique d'ordre n, alors ses générateurs sont les g^k pour $k \in \{1, \ldots, n\}$ premier avec n
- Prop : si G est d'ordre premier, alors G est cyclique

- Prop : si G est cyclique d'ordre n, alors pour tout diviseur $d \mid n$, il existe un unique sous-groupe d'ordre d de G, donné par $\{g \in G \mid g^d = 1\}$
- Thm de structure des groupes abéliens finis (admis)
- App : cyclicité de $\mathbb{F}_q^\times$

2.2. Étude du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ [Perrin]

- Def : indicatrice d'Euler
- Prop : $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$
- Prop : $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$
- Prop : si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \in \mathbb{N}^*$, alors $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times$
- Cor : $\varphi(n) = n\prod_{i=1}^r (1 - 1/p_i)$
- Thm : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique ssi :
  - $n = 4$
  - il existe p premier impair et $\alpha \in \mathbb{N}^*$ tels que $n = p^\alpha$ ou $n = 2p^\alpha$

3. Étude de groupes finis non abéliens

On fixe un entier $n \geq 2$.

3.1. Groupe symétrique

3.1.1. Définitions et résultats généraux [Rombaldi, Szpirglas]

- Def : $\mathfrak{S}_n$
- Prop : $|\mathfrak{S}_n| = n!$
- Thm : Cayley
- Prop : le centre de $\mathfrak{S}_n$ est égal à $\mathfrak{S}_n$ pour $n = 2$, et trivial pour $n \geq 3$
- Def : $\mathfrak{A}_n$
- Prop : $\mathfrak{A}_n$ est un sous-groupe d'indice 2 de $\mathfrak{S}_n$

3.1.2. Générateurs [Rombaldi, Szpirglas]

- Lemme : un r-cycle est produit de $r-1$ transpositions
- Thm : les éléments suivantes engendrent $\mathfrak{S}_n$:
  - les transpositions
  - les $(1 \quad i)$ pour $i \in \{1, \ldots, n\}$
  - les $(i \quad i+1)$ pour $i \in \{1, \ldots, n-1\}$
  - $(1 \quad 2)$ et $(1 \quad 2 \quad \cdots \quad n)$
- Rmq : comme $\mathfrak{S}_n$ n'est pas abélien (donc en particulier pas cyclique) lorsque $n \geq 3$, ce

dernier système a un nombre minimal de générateurs

- Lemme : si $i, j, k, \ell \in \{1, \dots, n\}$ sont distincts, alors :
  - $(i \quad j)\,(j \quad k) = (i \quad j \quad k)$
  - $(i \quad j)\,(k \quad \ell) = (i \quad j \quad k)\,(j \quad k \quad \ell)$
- Thm : $\mathfrak{A}_n$ est engendré par les 3-cycles
- Prop : les 3-cycles sont conjugués dans $\mathfrak{A}_n$ si $n \geq 5$

3.1.3. Structure de $\mathfrak{S}_n$ et $\mathfrak{A}_n$ [Perrin, Szpirglas]

- Thm : si $n \neq 4$, alors $\mathfrak{A}_n$ est simple
- Cor : si $n \geq 5$, alors $D(\mathfrak{A}_n) = \mathfrak{A}_n$ et $D(\mathfrak{S}_n) = \mathfrak{A}_n$
- Cor : si $n \neq 3$, alors les sous-groupes distingués non triviaux de $\mathfrak{S}_n$ sont $\mathfrak{A}_n$ et $\mathfrak{S}_n$
- Cor : un sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$

3.2. Groupe linéaire d'un corps fini [Perrin]

- Prop : cardinal de $\mathrm{GL}_n(\mathbb{F}_q)$ et associés
- Thm : isomorphismes exceptionnels

Annexe [Berhuy]

- Classification des groupes d'ordre ≤ 9