Développements :

- Simplicité du groupe alterné
- Isomorphismes exceptionnels

Références :

- Algèbre, Gourdon
- Algèbre - Tome 2 - Groupes, Szpirglas
- Anneaux, corps, résultants, Ulmer
- Mathématiques pour l'agrégation, Rombaldi

On fixe un entier $n \geq 2$.

1. Groupe symétrique

1.1. Permutations, cycles et transpositions [Rombaldi, Szpirglas]

- Def : ensemble des permutations $\mathfrak{S}(E)$ d'un ensemble E
- Prop : si E et F sont en bijection, alors $\mathfrak{S}(E) \cong \mathfrak{S}(F)$
- Def : groupe symétrique $\mathfrak{S}_n = \mathfrak{S}(\{1, \dots, n\})$
- Notation : $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$
- Def : on dit que $\sigma \in \mathfrak{S}_n$ est un r-cycle lorsqu'il existe une partie $\{x_1, \dots, x_r\} \subseteq \{1, \dots, n\}$ telle que :
  - $\sigma(x_k) = x_{k+1}$ pour tout $k \in \{1, \dots, r-1\}$
  - $\sigma(x_r) = x_1$
  - $\sigma(x) = x$ pour tout $x \notin \{x_1, \dots, x_r\}$

  et on le note alors $(x_1 \cdots x_r)$
- Def : une transposition est un 2-cycle
- Prop : si $\sigma \in \mathfrak{S}_n$ et $x_1, \dots, x_r \in \{1, \dots, n\}$, alors $\sigma(x_1 \cdots x_r)\sigma^{-1} = (\sigma(x_1) \cdots \sigma(x_r))$
- Prop : $|\mathfrak{S}_n| = n!$

1.2. Support et orbites [Rombaldi, Szpirglas]

- Def : support d'une permutation $\mathrm{supp}(\sigma) = \{k \in \{1, \dots, n\} \mid \sigma(k) \neq k\}$
- Ex : le support du cycle $(x_1 \cdots x_r)$ est $\{x_1, \dots, x_r\}$
- Prop : si $\sigma, \tau \in \mathfrak{S}_n$, alors :

    - $\sigma(\mathrm{supp}(\sigma)) = \mathrm{supp}(\sigma)$
    - $\mathrm{supp}(\sigma) = \mathrm{supp}(\sigma^{-1})$
    - $\mathrm{supp}(\sigma^r) \subseteq \mathrm{supp}(\sigma)$ pour tout $r \in \mathbb{Z}$
    - si $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \varnothing$, alors $\sigma\tau = \tau\sigma$
- Notation : $\mathrm{Orb}_\sigma(k)$ désigne l'orbite de k pour l'action $\langle\sigma\rangle \curvearrowright \{1, \dots, n\}$
- Lemme : $|\mathrm{Orb}_\sigma(k)|$ est le plus petit entier $r \in \mathbb{N}^*$ tel que $\sigma^r = \mathrm{id}$, et on a alors $\mathrm{Orb}_\sigma(k) = \{k, \sigma(k), \dots, \sigma^{r-1}(k)\}$
- Thm : toute permutation $\sigma \in \mathfrak{S}_n$ se décompose en produit de cycles à supports disjoints $c_1, \dots, c_p$, unique à l'ordre près, et :
    - $\mathrm{supp}(\sigma) = \mathrm{supp}(c_1) \cup \ldots \cup \mathrm{supp}(c_p)$
    - l'ordre de σ est le ppcm des ordres des c_i
- Ex : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 8 & 3 & 5 & 2 & 1 & 7 \end{pmatrix} = (1 \quad 4 \quad 3 \quad 8 \quad 7)\,(2 \quad 6)$

1.3. Systèmes de générateurs [Szpirglas]

- Lemme : tout r-cycle est produit de $r-1$ transpositions
- Thm : les éléments suivantes engendrent $\mathfrak{S}_n$:
    - les transpositions
    - les $(1 \quad i)$ pour $i \in \{1, \dots, n\}$
    - les $(i \quad i+1)$ pour $i \in \{1, \dots, n-1\}$
    - $(1 \quad 2)$ 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

2. Groupe alterné, signature

2.1. Signature d'une permutation [Szpirglasa]

- Def : une inversion de $\sigma \in \mathfrak{S}_n$ est un couple (i, j) d'éléments distincts $i, j \in \{1, \dots, n\}$ tels que $i < j$ et $\sigma(i) > \sigma(j)$
- Prop : l'application $\varepsilon : \mathfrak{S}_n \to \mathbb{C}^\times$ définie par $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$ est un morphisme de groupes
- Thm : c'est l'unique morphisme non trivial $\mathfrak{S}_n \to \mathbb{C}^\times$, appelé signature
- Cor : si $\sigma \in \mathfrak{S}_n$, alors $\varepsilon(\sigma) = (-1)^{\iota(\sigma)}$ où $\iota(\sigma)$ est le nombre d'inversions de σ
- Cor : la parité du nombre de transpositions entrant dans une décomposition d'une permutation est indépendante de cette décomposition
- Ex : la signature d'un r-cycle est $(-1)^{r-1}$

2.2. Groupe alterné [Szpirglas]

- Def : on dit que $\sigma \in \mathfrak{S}_n$ est paire (resp. impaire) lorsque $\varepsilon(\sigma) = 1$ (resp. $\varepsilon(\sigma) = -1$)
- Def : le groupe alterné $\mathfrak{A}_n$ est l'ensemble des permutations paires de $\mathfrak{S}_n$
- Ex : $\mathfrak{A}_3 = \{\mathrm{id}, (1\,2\,3), (1\,3\,2)\}$
- Prop : $\mathfrak{A}_n$ est un sous-groupe d'indice 2 de $\mathfrak{S}_n$
- 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 $n \geq 5$

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

- Prop : le centre de $\mathfrak{S}_n$ est égal à $\mathfrak{S}_n$ pour $n \leq 2$, et trivial pour $n \geq 3$
- 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. Applications

3.1. Construction du déterminant [Gourdon]

- Notation : $\mathscr{L}_p(E, K)$ désigne l'ensemble des formes p-linéaires sur E
- Prop : $\dim \mathscr{L}_p(E, K) = (\dim E)^p$
- Def : forme alternée, forme antisymétrique
- Thm : si K n'est pas de caractéristique 2, alors f est antisymétrique ssi f est alternée
- Prop : si $f \in \mathscr{L}_p(E, K)$ est alternée et $(x_1, \dots, x_p) \in E^p$ est liée, alors $f(x_1, \dots, x_p) = 0$
- Thm : si $\dim E = n$, alors l'ensemble des formes n-linéaires alternées sur E est une droite vectorielle, et si B est une base de E, alors il existe une unique forme n-linéaire alternée sur E pour laquelle l'image de B vaut 1
- Def : cette forme est appelée déterminant en base B et notée $\det_B$
- Prop : $\det_B(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}$ où $x_i = \sum_{j=1}^n x_{i,j} e_j$
- Thm : pour $x_1, \dots, x_n \in E$, s'équivalent :
  - $(x_1, \dots, x_n)$ est liée
  - $\det_B(x_1, \dots, x_n) = 0$ pour une certaine base B de E
  - $\det_B(x_1, \dots, x_n) = 0$ pour toute base B de E

3.2. Actions de groupes

3.2.1. Cadre théorique général [Rombaldi, Szpirglas]

- Def : une action $G \curvearrowright X$ est un morphisme de groupes $G \to \mathfrak{S}(X)$
- Ex : action naturelle $\mathfrak{S}_n \curvearrowright \{1, \dots, n\}$
- Thm (Cayley) : si G est un groupe, alors il est isomorphe à un sous-groupe de $\mathfrak{S}(G)$
- Notation : si $\sigma \in \mathfrak{S}_n$ et K est un corps, on note P_σ la matrice de passage de la base canonique $(e_1, \dots, e_n)$ de K^n à la base $(e_{\sigma(1)}, \dots, e_{\sigma(n)})$
- Prop : l'application $\mathfrak{S}_n \to \mathrm{GL}_n(K)$ définie par $\sigma \longmapsto P_\sigma$ est un morphisme de groupes injectif
- Thm : tout groupe fini d'ordre $n \in \mathbb{N}^*$ est isomorphe à un sous-groupe de $\mathrm{GL}_n(K)$

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

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

3.3. Polynômes symétriques [Gourdon, Ulmer]

- Def : on dit que $P \in A[X_1, \dots, X_n]$ est symétrique lorsque $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P$ pour toute permutation $\sigma \in \mathfrak{S}_n$
- Ex : $X^3 + Y^3 + Z^3 \in \mathbb{Z}[X, Y, Z]$ est symétrique
- Def : polynômes symétriques élémentaires $\Sigma_j = \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq n} X_{i_1} \cdots X_{i_j}$
- Ex : $\Sigma_1 = X_1 + \ldots + X_n$, $\Sigma_2 = \sum_{i<j} X_i X_j$, $\Sigma_n = X_1 \cdots X_n$
- Thm : si $P \in A[X_1, \dots, X_n]$ est symétrique, alors il existe un unique $Q \in A[X_1, \dots, X_n]$ tel que $P = Q(\Sigma_1, \dots, \Sigma_n)$
- Ex : dans $\mathbb{Z}[X, Y, Z]$, $X^3 + Y^3 + Z^3 = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3$