Leçon 105 - Groupe des permutations d'un ensemble fini. Applications.

Extrait du rapport de jury

Parmi les attendus, il faut savoir relier la leçon avec les notions d'orbites et d'actions de groupes. Il faut aussi savoir décomposer une permutation en cycles à supports disjoints, tant sur le plan théorique (preuve du théorème de décomposition), que pratique (sur un exemple) et savoir l'utiliser pour déterminer les classes de conjugaisons du groupe symétrique et pour donner des systèmes de générateurs. L'existence du morphisme signature est un résultat non trivial mais ne peut pas constituer, à elle seule, l'objet d'un développement. Il est bon d'avoir en tête que tout groupe fini se plonge dans un groupe symétrique et de savoir calculer la signature des permutations ainsi obtenues dans des cas concrets. Les applications sont nombreuses, il est très naturel de parler du déterminant, des polynômes symétriques ou des fonctions symétriques des racines d'un polynôme. On peut également parler du lien avec les groupes d'isométries des solides.
Pour aller plus loin, les candidates et candidats peuvent aller plus loin en s'intéressant par exemple aux automorphismes du groupe symétrique, à des problèmes de dénombrement, aux représentations des groupes des permutations ou encore aux permutations aléatoires.

Présentation de la leçon

Je vais vous présenter la leçon 105 intitulée : "Groupe des permutations d'un ensemble fini. Applications.". Le groupe $\mathfrak{S}_n$ est à l'origine de beaucoup de domaines, notamment de la théorie des groupes qui s'est par la suite généralisée ainsi que la théorie de Galois et la résolubilité des équations polynomiales avec les permutations de racines. Étudier la structure du groupe $\mathfrak{S}_n$ est intéressant car ce groupe intervient naturellement dans de nombreuses situations, comme nous allons le voir. De plus, l'isomorphisme canonique entre $\mathfrak{S}(E)$ et $\mathfrak{S}_n$ pour tout ensemble E de cardinal n et le théorème de Cayley rajoutent de l'attrait pour ce groupe.
Dans une première partie, on donne les généralités sur le groupe des permutations. On montre tout d'abord qu'il s'agit bien d'un groupe puis on donne ensuite quelques isomorphismes qui nous permettent d'identifier un groupe des permutations sur un ensemble quelconque à $\mathfrak{S}_n$. On parle ensuite des éléments de $\mathfrak{S}_n$ avec plus particulièrement les cycles. On commence par rappeler la définition d'un cycle ainsi que son ordre avant de définir le support ainsi que la σ-orbite qui nous permet de caractériser les cycles. On donne ensuite le théorème 15 ainsi que le corollaire 16 qui sont fondamentaux notamment pour calculer les puissances d'un cycle, son ordre ainsi que sa signature. On termine ce deuxième point avec des générateurs de $\mathfrak{S}_n$ ainsi que le dénombrement des dérangements. Dans un dernier point on parle des classes de conjugaison en introduisant la notion de type d'une permutation qui permet de donner une condition nécessaire et suffisante pour que deux cycles soient conjugués, mais qui permet également de dénombrer le nombre ainsi que le cardinal des classes de conjugaison. On parle enfin de la signature qui est l'unique morphisme de groupes non trivial de $\mathfrak{S}_n$ sur $\mathbb{C}^*$.
Dans une deuxième partie on s'intéresse aux sous-groupes remarquables ainsi qu'aux automorphismes de $\mathfrak{S}_n$. On commence par le groupe alterné qui est définit comme le noyau de la signature et on montre qu'il est simple pour $n \geq 5$, ce qui a une importance capitale dans la résolution des équations polynomiales en terme de résolubilité. Ce résultat nous permet de parler du centre ainsi que du groupe dérivé de $\mathfrak{S}_n$. En effet, on montre que le centre de $\mathfrak{S}_n$ et $\mathfrak{A}_n$ est trivial dès lors que $n \geq 3$ ou 4 et on donne le groupe dérivé de $\mathfrak{A}_n$ ainsi que les sous-groupes distingués de $\mathfrak{S}_n$. Dans un dernier point on donne les automorphismes de $\mathfrak{S}_n$ en montrant qu'ils sont tous intérieurs sauf lorsque $n = 6$ puis l'on étudie le cas $n = 6$.
Enfin dans une dernière partie on donne quelques applications en commençant par quelques isomorphismes exceptionnels avant de passer au cas des corps finis où l'on donne le théorème de Frobenius-Zolotarev. On continue ensuite avec un troisième point consacré aux théorèmes de Sylow, où l'intérêt est justifié par l'exemple 63 où l'on montre que $\mathfrak{A}_5$ est l'unique groupe simple d'ordre 60 à l'isomorphisme près. Dans un quatrième point on s'intéresse aux matrices de permutations qui permettent de plonger n'importe quel groupe dans $\mathrm{GL}_n(\mathbb{F}_p)$ grâce au théorème de Cayley et à la proposition 68. Et enfin on donne une dernière application en géométrie avec le groupe des isométries du cube, puis laissant invariant les 5 solides de Platon.
On trouvera également en annexe une illustration des solides de Platon ainsi qu'une

correspondance entre les éléments de $\mathfrak{S}_4$ et $\mathrm{Isom}^+(\mathcal{C})$.

Plan général

Cours détaillé

Dans toute cette leçon, on considère n un entier naturel non nul.

I Généralités

I.1 Groupe des permutations

Dans toute cette sous-partie, on considère un ensemble E à n éléments.

Définition 1 : Groupe des permutations [Rombaldi, p.37] :
On appelle **groupe des permutations de** E l'ensemble des bijections de E sur lui-même et on le note $\mathfrak{S}(E)$.

Proposition 2 : [Rombaldi, p.37]
L'ensemble $\mathfrak{S}(E)$ est un groupe pour la loi $\circ$.

Lemme 3 : [Rombaldi, p.39]
Soit F un ensemble non vide.
Si E et F sont en bijection, alors $\mathfrak{S}(E)$ et $\mathfrak{S}(F)$ le sont aussi.

Corollaire 4 : [Rombaldi, p.39]
Puisque E possède n éléments, on a $\mathfrak{S}(E) \cong \mathfrak{S}(\llbracket 1;n \rrbracket)$ (noté désormais $\mathfrak{S}_n$).

On utilise désormais l'identification entre $\mathfrak{S}(E)$ et $\mathfrak{S}_n$.

Proposition 5 : [Rombaldi, p.40]
On a $\mathrm{Card}(\mathfrak{S}_n) = n!$.

Pour $\sigma \in \mathfrak{S}_n$, on note $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.

Proposition 6 :
L'action naturelle de $\mathfrak{S}_n$ sur $\llbracket 1;n \rrbracket$ par permutation est fidèle et transitive.

I.2 Cycles

Définition 7 : r-cycle [Rombaldi, p.37] :
On considère $r \in \llbracket 0;n \rrbracket$.
On appelle **r-cycle** toute permutation $\sigma \in \mathfrak{S}_n$ qui permute circulairement r éléments de $\llbracket 1;n \rrbracket$ et laisse fixe les autres.

Pour les r-cycles, on utilisera l'écrire plus compact $\sigma = (x_1 \; x_2 \; \cdots \; x_r)$ qui est moins lourde.

Proposition 8 : [Rombaldi, p.38]
Soit $r \in [\![1;n]\!]$.
$*$ Un r-cycle est d'ordre r.
$*$ Les r-cycles sont tous conjugués entre eux et en particulier pour tout $\sigma \in \mathfrak{S}_n$, on a $\sigma(x_1\ x_2\ \cdots\ x_n)\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ \cdots\ \sigma(x_n))$.

Définition 9 : Support d'une permutation [Rombaldi, p.40] :
On considère $\sigma \in \mathfrak{S}_n$.
On appelle **support de** σ l'ensemble $\mathrm{Supp}(\sigma) = \{x \in [\![1;n]\!] \text{ tq } \sigma(x) \neq x\}$.

Proposition 10 : [Rombaldi, p.40]
Soient $\sigma, \sigma' \in \mathfrak{S}_n$.
$*$ $\sigma(\mathrm{Supp}(\sigma)) = \mathrm{Supp}(\sigma)$.
$*$ $\forall k \in \mathbb{Z}$, $\mathrm{Supp}\left(\sigma^k\right) = \mathrm{Supp}(\sigma)$ et en particulier $\mathrm{Supp}\left(\sigma^{-1}\right) = \mathrm{Supp}(\sigma)$.
$*$ Si $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \emptyset$, alors σ et σ' commutent.

Définition 11 : σ-orbite [Rombaldi, p.41] :
On considère $\sigma \in \mathfrak{S}_n$ et $x \in [\![1;n]\!]$.
On appelle **σ-orbite** l'ensemble $\mathrm{Orb}_\sigma(x) = \left\{\sigma^k(x),\ x \in [\![1;n]\!]\right\}$.

Remarque 12 : [Rombaldi, p.41]
$*$ Les σ-orbites forment une partition de $[\![1,n]\!]$.
$*$ Les σ-orbites non réduites à un point forment une partition du support.

Proposition 13 : [Rombaldi, p.41]
Si $\mathrm{Card}(\mathrm{Orb}_\sigma(x)) = r$, alors r est le plus petit entier naturel i tel que $\sigma^i(x) = x$ et on a $\mathrm{Orb}_\sigma(x) = \left\{x, \sigma(x), ..., \sigma^{r-1}(x)\right\}$.

Remarque 14 : [Rombaldi, p.42]
La restriction de σ sur chacune des σ-orbites est un cycle, en particulier une permutation est un cycle si, et seulement si, elle n'a qu'une seule σ-orbite non réduite à un point.

Théorème 15 : [Berhuy, p.204]
Toute permutation de $\mathfrak{S}_n$ se décompose en produit de cycles à supports disjoints et cette décomposition est unique à l'ordre des facteurs près.

Corollaire 16 : [Berhuy, p.208]
L'ordre d'une permutation est le PPCM des longueurs des cycles à supports disjoints qui la composent.

Exemple 17 :
On considère $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 5 & 1 & 2 & 7 & 8 & 6 \end{pmatrix}$.
On a alors $\sigma = (1\ 4)(2\ 3\ 5)(6\ 7\ 8)$ et $o(\sigma) = \mathrm{PPCM}(2,3,3) = 6$.

Proposition 18 : [Berhuy, p.212 + 213]
Le groupe $\mathfrak{S}_n$ est engendré par chacune des familles suivantes :
$*$ Les cycles. $*$ Les transpositions. $*$ Les transpositions $(1\ i)$ pour $i \in [\![2;n]\!]$.
$*$ Les transpositions $(i\ i+1)$ pour $i \in [\![1;n-1]\!]$. $*$ $(1\ 2)$ et $(1\ 2\ ...\ n)$.

Théorème 19 : [Berhuy, p.714]
Soit D_n le nombre de dérangements de $\mathfrak{S}_n$ (c'est-à-dire de permutations sans points fixes).
Pour tout entier naturel n, on a $n! = \sum_{k=0}^n \binom{n}{k} D_{n-k}$ et $D_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$.

Proposition 20 : [Caldero (1), p.239]
Soit $\mathbb{P}$ la probabilité uniforme sur $(\mathfrak{S}_n, \mathcal{P}(\mathfrak{S}_n))$.
Si F_n est la variable aléatoire réelle qui compte le nombre de points fixe de $\sigma \in \mathfrak{S}_n$, alors pour tout $r \in [\![0;n]\!]$ on a $\mathbb{P}(F_n = r) = \frac{\binom{n}{r} D_{n-r}}{\mathrm{Card}(\mathfrak{S}_n)} = \frac{1}{r!} \sum_{k=0}^{n-r} \frac{(-1)^k}{k!}$.
De plus, $(F_n)_{n \in \mathbb{N}^*}$ converge en loi vers la variable aléatoire Z qui suit une loi de Poisson de paramètre 1 et on a $\mathbb{E}(F_n) = \mathrm{Var}(F_n) = 1$.

I.3 Classe de conjugaison et signature

Définition 21 : Type d'une permutation [Berhuy, p.211] :
On considère $\sigma \in \mathfrak{S}_n$.
On appelle **type de** σ la liste $\lambda(\sigma) = [\lambda_1, ..., \lambda_n]$ où λ_1 est le nombre de points fixes de σ et λ_k le nombre de k-cycles dans la décomposition de σ.

Théorème 22 : [Berhuy, p.211]
Deux permutations de $\mathfrak{S}_n$ sont conjuguées si, et seulement si, elles ont le même type.

Proposition 23 : [Berhuy, p.212]
Le nombre total de classes de conjugaison dans le groupe symétrique $\mathfrak{S}_n$ est donné par $P(n) = \mathrm{Card}\left(\left\{[\lambda_1, ..., \lambda_n] \text{ tq } \lambda_1, ..., \lambda_n \in \mathbb{N} \text{ et } \sum_{k=1}^n k\lambda_k = n\right\}\right)$.

Exemple 24 : [Berhuy, p.212]
$\mathfrak{S}_4$ possède 5 classes de conjugaison distinctes puisque l'on a les décompositions suivantes : $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$ et elles sont respectivement représentées par $(1\ 2\ 3\ 4)$, $(1\ 2\ 3)$, $(1\ 2)$, $(1\ 2)(3\ 4)$ et $\mathrm{Id}_{[\![1;n]\!]}$.

Proposition 25 :
Soient $\sigma \in \mathfrak{S}_n$ et $[\lambda_1, ..., \lambda_n]$ son type.
On a $\mathrm{Card}(\{\rho \in \mathfrak{S}_n \text{ tq } \rho\sigma\rho^{-1} = \sigma\}) = \prod_{k=1}^n \lambda_k! k^{\lambda_k}$. Il y a $\left(\frac{n}{\prod_{k=1}^n \lambda_k! k^{\lambda_k}}\right)$ éléments dans la classe de conjugaison de σ.

Exemple 26 :
Comme un r-cycle a pour type $[\lambda_1, ..., \lambda_r, ..., \lambda_n] = [n-r, 0, ..., 0, 1, 0, ..., 0]$, il y a $\frac{n!}{r!(n-r)!}$ r-cycles dans $\mathfrak{S}_n$.

Définition 27 : Signature [Berhuy, p.213] :
Il existe un unique morphisme de groupes $\varepsilon : \mathfrak{S}_n \longrightarrow \mathbb{C}^\times$ non trivial appelé **signature** tel que pour toute transposition σ, $\varepsilon(\sigma) = -1$ et pour toute permutation ρ qui s'écrit comme produit de s transpositions, on a $\varepsilon(\rho) = (-1)^s$.

Proposition 28 : [Berhuy, p.214]
Soit $\sigma \in \mathfrak{S}_n$.
* Si σ est un r-cycle, on a $\varepsilon(\sigma) = (-1)^{r-1}$.
* Si σ a pour type $[\lambda_1, ..., \lambda_n]$, alors $\varepsilon(\sigma) = \prod_{i=1}^n (-1)^{\lambda_i(i-1)}$.

Exemple 29 :
Avec σ de l'exemple 17 on a $\varepsilon(\sigma) = -1$.

Théorème 30 : [Rombaldi, p.48]
Pour tout $\sigma \in \mathfrak{S}_n$, on a $\varepsilon(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i}$.

Remarque 31 : [Rombaldi, p.48]
ε compte donc le nombre d'inversions dans une permutation donnée.

II Sous-groupes remarquables et automorphismes

II.1 Le groupe alterné

Définition 32 : Groupe alterné [Berhuy, p.215] :
On appelle **groupe alterné** (noté $\mathfrak{A}_n$) le noyau du morphisme signature.

Proposition 33 : [Berhuy, p.215]
$\mathfrak{A}_n$ est l'unique sous-groupe distingué de $\mathfrak{S}_n$ et $\mathrm{Card}(\mathfrak{A}_n) = \frac{n!}{2}$.

Remarque 34 : [Berhuy, p.301 + 302]
On a $\mathfrak{S}_n = \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$.
Autrement dit, on a la suite exacte scindée :

$$\begin{tikzcd} \{\mathrm{Id}_{[\![1;n]\!]}\} \arrow[r] & \mathfrak{A}_n \arrow[r, "\iota"] & \mathfrak{S}_n \arrow[r, "\varepsilon"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[l, bend left, "s"] & \{\mathrm{Id}_{[\![1;n]\!]}\} \end{tikzcd}$$

Théorème 35 : [Rombaldi, p.49]
Les 3-cycles engendrent $\mathfrak{A}_n$ pour $n \geq 3$.

Développement 1 : [cf. ROMBALDI]

Théorème 36 : Simplicité de $\mathfrak{A}_n$ pour $n = 3$ ou $n \geq 5$ [Rombaldi, p.50] :
Pour $n = 3$ ou $n \geq 5$, le groupe $\mathfrak{A}_n$ est simple.

Remarque 37 : [Berhuy, p.219 + Perrin, p.28 + 37]
* En réalité, $\mathfrak{A}_5$ est le plus petit groupe simple non abélien (et tout groupe simple d'ordre 60 est isomorphe à $\mathfrak{A}_5$).
* Ce résultat est cohérent avec le théorème de Feit-Thompson (tout groupe simple fini et non abélien est d'ordre pair).
* Ce résultat a une importance historique majeure car il permet de montrer que pour $n \geq 5$, $\mathfrak{A}_n$ n'est pas résoluble et donc que les solutions des équations polynomiales de degré supérieur ou égal à 5 ne peuvent s'écrire à l'aide des quatre opérations élémentaires et de la racine carré.

Remarque 38 : [Perrin, p.30]
* Si $n = 4$, alors $\mathfrak{A}_n$ n'est pas simple car contient comme sous-groupe distingué $H = \left\{\mathrm{Id}_{[\![1;4]\!]}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\right\}$.
* De plus, $\mathfrak{A}_4$ est le plus petit groupe (à l'isomorphisme près) qui ne vérifie pas la réciproque du théorème de Lagrange.

Proposition 39 : [Francinou, p.71]
Il existe un plongement de $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+2}$, mais pas dans $\mathfrak{A}_{n+1}$.

II.2 Centre et groupe dérivé

Proposition 40 : [Berhuy, p.219]
* Si $n \geq 3$, alors le centre de $\mathfrak{S}_n$ est trivial.
* Si $n \geq 4$, alors le centre de $\mathfrak{A}_n$ est trivial.

Corollaire 41 : [Perrin, p.28]
Pour $n \geq 5$, on a $D(\mathfrak{A}_n) = \mathfrak{A}_n$.

Corollaire 42 : [Berhuy, p.220 + Delcourt p.139]
* Si $n \geq 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont exactement $\mathrm{Id}_{[\![1;n]\!]}, \mathfrak{A}_n$ et $\mathfrak{S}_n$ et on a $D(\mathfrak{A}_n) = \mathfrak{A}_n$.
* De plus, on a $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

Remarque 43 : [Berhuy, p.220]
Si $n = 4$, alors il faut rajouter à la liste précédente le sous-groupe H de $\mathfrak{S}_4$ (cf. remarque 38).

II.3 Automorphismes du groupe symétrique

On note, pour tout $i \in [\![1;n]\!]$, $\mathfrak{S}_n(i) = \{\sigma \in \mathfrak{S}_n \text{ tq } \sigma(i) = i\}$.

Lemme 44 : [Perrin, p.30]
Soit H un sous-groupe d'indice n de $\mathfrak{S}_n$.
* H est isomorphe à $\mathfrak{S}_{n-1}$.
* Si $n \geq 2$, alors il existe $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$ tel que $\varphi(H) = \mathfrak{S}_n(1)$.

Lemme 45 : [Perrin, p.31]
Un automorphisme $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$ est intérieur si, et seulement si, l'image de chaque transposition est une transposition.

Théorème 46 : [Perrin, p.30]
Si $n \neq 6$, alors $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.

Proposition 47 : [Perrin, p.30]
* Si $n \in \{1;2\}$, alors $\mathrm{Aut}(\mathfrak{S}_n) = \left\{\mathrm{Id}_{[\![1;n]\!]}\right\}$.
* Si $n \geq 3$ et $n \neq 6$, on a $\mathrm{Aut}(\mathfrak{S}_n) \cong \mathfrak{S}_n$.

Proposition 48 : [Perrin, p.33]
Les assertions suivantes sont équivalentes :
* Les seuls-sous-groupes d'indice n de $\mathfrak{S}_n$ sont les $\mathfrak{S}_n(i)$.
* $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.

Corollaire 49 :
Les sous-groupes d'indice n de $\mathfrak{S}_n$ sont exactement les $\mathfrak{S}_n(i)$ lorsque $n \neq 6$.

Proposition 50 : [Perrin, p.33]
On a $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.
De plus, le groupe $\mathrm{Int}(\mathfrak{S}_6)$ est d'indice 2 (donc distingué) dans $\mathrm{Aut}(\mathfrak{S}_6)$.

Corollaire 51 :
On a $\mathrm{Card}(\mathrm{Aut}(\mathfrak{S}_6)) = 1440$.

III Applications

III.1 Quelques isomorphismes exceptionnels

Proposition 52 : [Perrin, p.106]
On a $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$.

Théorème 53 : [Perrin, p.106]
On a les isomorphismes suivants :
* $\mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$ et $\mathrm{PSL}_2(\mathbb{F}_3) \cong \mathfrak{A}_4$. * $\mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$.
* $\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$ et $\mathrm{PSL}_2(\mathbb{F}_5) \cong \mathfrak{A}_5$.

III.2 Sur un corps fini...

Théorème 54 : [Rombaldi, p.428]
Soit p un nombre premier.
Pour tout $a \in \mathbb{F}_p^*$, on a $a^{\frac{p-1}{2}} = \overline{\left(\frac{a}{p}\right)}$ dans $\mathbb{F}_p^*$ et l'application $a \longmapsto \left(\frac{a}{p}\right)$ est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ dans $\{-1;1\}$.

Corollaire 55 : [Rombaldi, p.429]
Soient $n \in \mathbb{N}^*$ et p un nombre premier impair.
L'application :
$$\Psi : \left| \begin{array}{ccc} \mathrm{GL}_n(\mathbb{F}_p) & \longrightarrow & \{-1;1\} \\ A & \longmapsto & \left(\frac{\det(A)}{p}\right) \end{array} \right.$$
est l'unique morphisme de groupes non trivial de $\mathrm{GL}_n(\mathbb{F}_p)$ dans $\{-1;1\}$.

Théorème 56 : Théorème de Frobenius-Zolotarev [Rombaldi, p.430] :
Soient $n \in \mathbb{N}^*$ et p un nombre premier impair.
Pour tout $A \in \mathrm{GL}_n(\mathbb{F}_p)$ on a $\varepsilon(A) = \left(\frac{\det(A)}{p}\right)$.

III.3 Actions de groupes et théorie de Sylow

Dans toute cette sous-partie, on considère E un ensemble quelconque non vide ainsi que $(G, *)$ un groupe.

Remarque 57 : [Berhuy, p.170]
La donnée d'une action de G sur E est équivalente à la donnée d'un morphisme de groupes de G dans $\mathfrak{S}_E$. En effet, G agit sur E via $\cdot$ si, et seulement si, l'application
$$\Psi : \left| \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}_E \\ g & \longmapsto & \sigma_g : \left| \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & g \cdot x \end{array} \right. \end{array} \right.$$
est un morphisme de groupes.

Théorème 58 : Théorème de Cayley [Berhuy, p.177] :
Si G est d'ordre n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

On suppose jusqu'à la fin de cette sous-partie, que $(G,*)$ est un groupe de cardinal fini noté n et p un nombre premier.

Définition 59 : p-sous-groupe de G [Berhuy, p.311] :
On appelle **p-sous-groupe de** G tout sous-groupe de G de cardinal une puissance de p.

Désormais, on écrit $\mathrm{Card}(G) = n = p^m q$ où $p \nmid q$ et $m \in \mathbb{N}^*$.

Définition 60 : p-sous-groupe de Sylow de G [Berhuy, p.311] :
On appelle **p-sous-groupe de Sylow de** G (ou plus simplement p-Sylow) tout sous-groupe de G d'ordre p^m.

Exemple 61 :
* $\mathbb{Z}/6\mathbb{Z}$ contient un 2-Sylow et un 3-Sylow (respectivement $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$).
* $\mathbb{Z}/56\mathbb{Z}$ contient un 2-Sylow et un 7-Sylow (respectivement $\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$).

Théorème 62 : Théorème de Sylow [Berhuy, p.313] :
* Il existe des p-sous-groupes de Sylow de G et tout p-sous-groupe de G est contenu dans un p-Sylow.
* Le conjugué d'un p-Sylow est un p-Sylow et tous les p-Sylow de G sont conjugués entre eux. En particulier, si S est un p-Sylow de G, alors S est distingué dans G si, et seulement si, S est l'unique p-Sylow de G.
* Si n_p désigne le nombre de p-Sylow de G, alors $n_p \equiv 1$ $[p]$ et $n_p | q$.

Exemple 63 : [Berhuy, p.219]
* $\mathfrak{A}_5$ est l'unique groupe simple d'ordre 60 à l'isomorphisme près.
* Tout sous-groupe de $\mathfrak{S}_4$ d'ordre 8 est isomorphe à D_8.

Théorème 64 : Théorème de Cauchy [Berhuy, p.179] :
G possède au moins un élément d'ordre p.

III.4 Matrices de permutation

Définition 65 : Matrice de permutation [Rombaldi, p.54] :
On considère $\sigma \in \mathfrak{S}_n$.
On appelle **matrice de permutation associée à** σ la matrice $(P_\sigma)_{i,j} = \delta_{i,\sigma(j)}$.

Remarque 66 :
Ces matrices sont essentiellement utilisées lorsque l'on résout des systèmes linéaires avec la méthode du pivot de Gauss.

Proposition 67 : [Rombaldi, p.54]
L'application :

$$\Psi : \left| \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \mathrm{GL}_n(\mathbb{F}_p) \\ \sigma & \longmapsto & P_\sigma \end{array} \right.$$

est un morphisme de groupes injectif et $\det(P_\sigma) = \varepsilon(\sigma)$.

Proposition 68 : [Rombaldi, p.158]
Soit $(G,*)$ un groupe.
Si G est d'ordre n, alors pour tout nombre premier p, G est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$.

III.5 Groupe des isométries

On fixe un espace affine euclidien $\mathcal{E}$ de dimension 3.
On considère un cube $\mathcal{C}$ de côté $c > 0$ comme l'ensemble de ses sommets.

Théorème 69 : [Combes, p.147]
L'ensemble des polyèdres réguliers de $\mathcal{E}$ sont à similitude près le tétraèdre régulier, le cube, l'octaèdre régulier, le dodécaèdre régulier et l'icosaèdre régulier.

Développement 2 : [cf. COMBES]

Théorème 70 : [Combes, p.175]
On a $\mathrm{Isom}^+(\mathcal{C}) \cong \mathfrak{S}_4$ et $\mathrm{Isom}(\mathcal{C}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

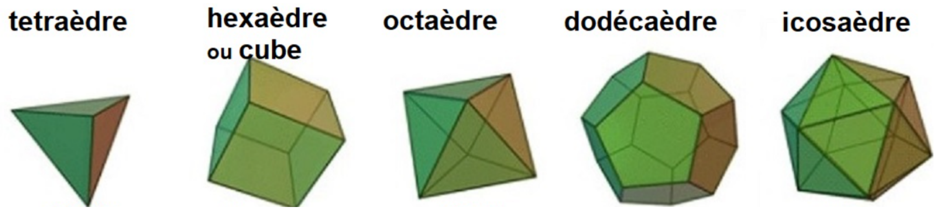
Remarque 71 :
On donne en annexe une correspondance entre les éléments de $\mathfrak{S}_4$ et de $\mathrm{Isom}^+(\mathcal{C})$.

Théorème 72 : [Caldero (2), p.222 + 227]
* On a $\mathrm{Isom}^+(\mathcal{T}) \cong \mathfrak{A}_4$ et $\mathrm{Isom}(\mathcal{T}) \cong \mathfrak{S}_4$.
* On a $\mathrm{Isom}^+(\mathcal{O}) \cong \mathfrak{S}_4$ et $\mathrm{Isom}(\mathcal{O}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.
* On a $\mathrm{Isom}^+(\mathcal{D}) \cong \mathrm{Isom}^+(\mathcal{I}) \cong \mathfrak{A}_5$ et $\mathrm{Isom}(\mathcal{D}) \cong \mathrm{Isom}(\mathcal{I}) \cong \mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$.

Théorème 73 : [Combes, p.171]
Les sous-groupes finis de $\mathrm{Isom}^+(\mathcal{E})$ sont exactement à isomorphismes près :
* Le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$. * Le groupe diédral D_{2n}.
* Les groupes $\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathfrak{A}_5$.

IV Annexe

IV.1 Solides de Platon



IV.2 Correspondance entre les éléments de $\mathfrak{S}_4$ et $\text{Isom}^+(\mathcal{C})$

$\mathcal{S}_4$	$\text{Isom}^+(\mathcal{C})$	Cardinal
$\text{Id}_{[\![1;n]\!]}$	Identité	1
(1 2)	Rotation d'axe passant par les milieux de deux arêtes opposées et d'angle $\pm\pi$	6
(1 2 3)	Rotation d'axe une grande diagonale et d'angle $\pm\frac{2\pi}{3}$	8
(1 2 3 4)	Rotation d'axe passant par les centres de deux faces opposées et d'angle $\pm\frac{\pi}{2}$	6
(1 2)(3 4)	Rotation d'axe passant par les centres de deux faces opposées et d'angle $\pm\pi$	3

Remarques sur le plan

- Il est important de donner un contexte historique à l'apparition de $\mathfrak{S}_n$ et de justifier son intérêt en montrant en quoi la connaissance de ce groupe si riche apporte tant d'informations pour d'autres groupes et surtout dans d'autres domaines.
- Il faut savoir décomposer une permutation en produit de cycles à supports disjoints et de calculer des puissances de cycles.
- Il est bon de connaître les morphismes de $\mathfrak{S}_n$ dans $\mathfrak{S}_{n-1}$.
- On peut également parler du déterminant, des polynômes (semi-)symétriques ainsi que de tables de caractères.

Liste des développements possibles

- Simplicité de $\mathfrak{A}_n$ pour $n = 3$ ou $n \geq 5$.
- Groupe des isométries du cube.

Bibliographie

- Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et Géométrie*.
- Grégory Berhuy, *Algèbre : le grand combat*.
- Philippe Caldero, *Carnet de voyage en Analystan*.
- Daniel Perrin, *Cours d'algèbre*.
- Serge Francinou, *Exercices de mathématiques, Oraux X-ENS, Algèbre 1*.
- Jean Delcourt, *Théorie des groupes*.
- François Combes, *Algèbre et géométrie*.
- Philippe Caldero, *Nouvelles histoires hédonistes de groupes et de géométries, tome 2*.