2) Générateurs de S_n et de A_n

Proposition 21: S_n est engendré par:
(1) Les cycles
(2) Les transpositions
(3) Les transpositions de la forme $(1\ k)$ avec $k \in [\![2;n]\!]$
(4) Les transpositions de la forme $(k\ k{+}1)$ avec $k \in [\![1;n-1]\!]$
(5) $(1\ 2)$ et $(1\ 2 \cdots n)$

Exemple 22:
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1\ 2\ 3\ 4\ 5)(6\ 7)$$
$$= (1\,2)(2\,3)(3\,4)(4\,5)(6\,7)$$
$$= (1\,3)(1\,2)(1\,3)(1\,4)(1\,3)(1\,4)(1\,5)(1\,4)(1\,6)(1\,7)(1\,6)$$

Proposition 23: A_n est engendré par: (pour $n \geq 3$)
(1) Les 3-cycles
(2) Les 3-cycles de la forme $(1\ 2\ k)$ avec $k \in [\![3;n]\!]$
(3) Les 3-cycles de la forme $(k\ k{+}1\ k{+}2)$ avec $k \in [\![1;n-2]\!]$.

Application 24: Pour $n=3$ et $n \geq 5$, A_n est simple

Application 25: Les sous-groupes normaux de S_n sont S_n, A_n et $\{e\}$.

III) Quelques applications du groupe symétrique

1) Théorème de Frobenius-Zolotarev

Définition 26: Une matrice de dilatation de $GL_n(\mathbb{K})$ est une matrice de la forme $\mathrm{diag}(1;\dots;1;\lambda)$ avec $\lambda \in \mathbb{K}^*$.
Étant donné H et G deux espaces supplémentaires tels que: H est un hyperplan, la dilatation f de base H, direction G et de rapport $\lambda \in \mathbb{K}^*$ est l'unique endomorphisme tel que pour tout $x, y \in H \times G$, $f(x+y) = x + \lambda y$

Lemme 27: Soit $u \in GL(E)$ et H hyperplan de E tel que $u_{|H} = id$ et $\det(u) \neq 1$
Alors: u est une dilatation

Définition 28: Soit $u \in GL(E)$, H hyperplan de E. On dit que u est une transvection d'hyperplan H si $u_{|H} = id_H$, $u \neq id$ et $\det(u) \neq 1$.

Théorème 29: Soit $\mathbb{K}$ à au moins 3 éléments.
Alors: Les dilatations engendrent $GL(E)$.

Lemme 30: (1) L'application $\varphi : \begin{array}{l} \mathbb{F}_p^* \to \{\pm 1\} \\ a \mapsto \left(\frac{a}{p}\right) \end{array}$ est un morphisme de groupes.
(2) Soit p premier impair, alors: il y a $\frac{p-1}{2}$ résidus modulo $p-1$.

Théorème 31: Soit $\mathbb{K}$ corps fini
Alors: il existe $a \in \mathbb{K}^*$ tel que $\mathbb{K}^* = \langle a \rangle$.

Théorème 32: (de Frobenius-Zolotarev) Soit p premier impair, V un $\mathbb{F}_p$-ev de dimension n.
Alors: pour tout $u \in GL(V)$, $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$

2) Décomposition de Bruhat

Définition 33: Un drapeau est une suite croissante (pour l'inclusion) d'espaces vectoriels $(A_0;\dots;A_n)$. On note $\mathcal{D}$ l'ensemble des drapeaux de E.
Pour la base canonique $(e_1;\dots;e_n)$, on note $S = (\mathrm{Vect}(e_1;\dots;e_i))_{i=0}^{n}$ le drapeau canonique de E.

Notation 34: On note T_s l'ensemble des matrices triangulaires supérieures de taille n.

Théorème 35: (décomposition de Bruhat) $GL_n(\mathbb{K}) = \bigsqcup_{\sigma \in S_n} T_s P_\sigma T_s$ avec P_σ une matrice dont on a permuté les colonnes de la matrice identité I_n par σ.

105

Groupe de permutation d'un ensemble fini. Applications.

Soit $n \geq 2$ et E ensemble de cardinal n.

I| Groupe de permutations

1| Éléments de S_n

[Rom] I.1

Définition 1 : Le groupe des permutations de E, noté $S(E)$, est le groupe des bijections de E dans E.

Pour $E = [\![1;n]\!]$, on note $S_n = S(E)$ le groupe symétrique à n éléments.

I.1

Proposition 2 : $(S_n ; \circ)$ est un groupe d'ordre $n!$ de neutre e la permutation identitée.

Notation 3 : On note $\sigma \in S_n$ sous la forme $\sigma = \begin{pmatrix} 1 & 2 & - & n \\ \sigma(1) & \sigma(2) & - & \sigma(n) \end{pmatrix}$.

Exemple 4 : Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ et $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ deux permutations de S_3.

On a $\sigma \circ \rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $\rho \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

En particulier, S_3 est non-abélien.

[Ulm]

Proposition 5 : S_n agit naturellement sur $[\![1;n]\!]$ par permutation et a pour morphisme structurel $\varphi : \begin{array}{rcl} S_n & \longrightarrow & S([\![1;n]\!]) \\ \sigma & \longmapsto & \begin{array}{rcl} [\![1;n]\!] & \longrightarrow & [\![1;n]\!] \\ i & \longmapsto & \sigma \cdot i = \sigma(i) \end{array} \end{array}$

II.2

Théorème 6 : (de Cayley) Tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n.

Remarque 7 : Ce théorème a ses limites. En effet, $GL_2(\mathbb{F}_2)$ est d'ordre 6 et est alors isomorphe à un sous-groupe de S_6 qui a 720 éléments. Il est bien plus intéressant de noter que $GL_2(\mathbb{F}_2) \simeq S_3$.

2| Orbites et cycles

I.1

Définition 8 : Soit $\sigma \in S_n$. Les éléments $i \in [\![1;n]\!]$ qui vérifient $\sigma(i) = i$ sont appelés points fixes de la permutation σ.

L'ensemble $[\![1;n]\!]$ privé des points fixes de σ est appelé support de σ.

[Ulm]

Proposition 9 : Soit $\sigma, \rho \in S_n$ telles que $Supp(\sigma) \cap Supp(\rho) = \emptyset$.

Alors : $\sigma \circ \rho = \rho \circ \sigma$ et $Supp(\sigma \circ \rho) = Supp(\sigma) \cup Supp(\rho)$

Définition 10 : Soit $\ell \in \mathbb{N}^*$ et $i_1 ; \dots ; i_\ell \in [\![1;n]\!]$ distincts. La permutation $\gamma \in S_n$ définie par $\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1 ; \dots ; i_\ell\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k < \ell \\ i_1 & \text{si } j = i_\ell \end{cases}$ est appelée cycle de longueur ℓ.

Elle est notée $(i_1 \; i_2 \cdots i_\ell)$. Un cycle de longueur 2 est appelé une transposition.

I.1

Proposition 11 : Un r-cycle est d'ordre r dans $(S_n ; \circ)$.

Proposition 12 : $Z(S_n) = \begin{cases} S_n & \text{si } n = 2 \\ \{e\} & \text{si } n \geq 3 \end{cases}$

I.4 [Rom]

Théorème 13 : Toute permutation $\sigma \in S_n \setminus \{e\}$ se décompose en produit de cycles 2 à 2 disjoints de manière unique à l'ordre près. Si $\sigma = \gamma_1 \circ \dots \circ \gamma_p$ est une telle décomposition, alors : $Supp(\sigma) = \bigcup_{k=1}^{p} Supp(\gamma_k)$ et $ord(\sigma) = PPCM(ord(\gamma_1) ; \dots ; ord(\gamma_p))$.

Exemple 14 : Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$, on a deux cycles $(1\,2\,3\,4\,5)$ et $(6\;7)$ et deux points fixes d'où : $\sigma = (1\,2\,3\,4\,5)(6\,7)$

II| Groupe alterné A_n et structure de A_n et de S_n

1| Groupe alterné A_n

I.3

Définition 15 : La signature de $\sigma \in S_n$ est : $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$

Proposition 16 : L'application $\varepsilon : S_n \to (\mathbb{Q}^* ; \cdot)$ qui à une permutation associe sa signature est un morphisme de groupes.

[Ulm]

Propriétés 17 : Soit $\sigma \in S_n$.

Alors : (1) Si σ est une transposition, alors $\varepsilon(\sigma) = -1$.

(2) Si $\sigma = \gamma_1 \circ \dots \circ \gamma_m$ est une décomposition en produit de cycles de longueurs $\ell_1 ; \dots ; \ell_m$, alors $\varepsilon(\sigma) = \prod_{i=1}^{m} (-1)^{\ell_i - 1}$.

(3) L'image du morphisme ε est le sous-groupe $\{-1 ; 1\}$ de $\mathbb{Q}^*$.

Définition 18 : Le noyau du morphisme $\varepsilon : S_n \to \{\pm 1\}$ est un sous-groupe normal de S_n appelé sous-groupe alterné A_n.

Proposition 19 : $A_n \lhd S_n$ et $|A_n| = \frac{n!}{2}$.

Exemple 20 : $A_4 = \{e ; (12)(34) ; (13)(24) ; (14)(23) ; (132) ; (143) ; (234) ; (124) ; (134) ; (142) ; (243) ; (123)\}$

Références:

[Rom] Mathématiques pour l'agrégation Algèbre et Géométrie - Rombaldi
[Ulm] Théorie des groupes - Ulmer
[Isen] L'oral à l'agrégation de mathématiques - Isenmann