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

1. Généralités sur le groupe symétrique. —

1. Définition et propriétés. —

- Def : Pour tout $n \geq 1$, on note Σ_n le groupe des bijections de $\{1,..,n\}$, appelé n-ième groupe symétrique.
- Pro : Σ_n est un groupe, de cardinal $Card(\Sigma_n) = n!$.
- Not : On peut représenter $\sigma \in \Sigma_n$ par la matrice $\begin{pmatrix} 1 & .. & n \\ \sigma(1) & .. & \sigma(n) \end{pmatrix}$
- Rem : Pour tout $1 \leq i \leq n$, pour tous $\sigma, \tau \in \Sigma_n$, $\sigma.\tau(i) = \sigma(\tau(i))$.
- Rem : Pour E un ensemble fini de cardinal n, on peut faire agir Σ_n sur E en numérotant les éléments de E.
- Pro : Pour tout $m \leq n$, on a un isomorphisme de groupes $\bigcap_{i \leq m+1}^{n} Stab_{\Sigma_n}(i)$ et Σ_m. On a ainsi un morphisme injectif de Σ_m dans Σ_n.
- Pro : Soit G un groupe fini de cardinal n. L'application $g \in G \mapsto (x \mapsto g.x.g^{-1}) \in Bij(G)$ est un morphisme de groupes injectif.
  On a ainsi un sous-groupe de Σ_n isomorphe à G.
- Théorème de Cayley : L'image de G par $g \mapsto (x \mapsto g.x.g^{-1})$ est un sous-groupe transitif de Σ_n.
- Def : Soit K un corps et B la base canonique de K^n. Pour tout $\sigma \in \Sigma_n$ on définit T_σ la matrice dont le coefficient (i,j) vaut 1 si $i = \sigma(j)$ et 0 sinon, et on l'appelle matrice de permutation associée à σ.
- Pro : $\sigma \in \Sigma_n \mapsto T_\sigma \in Gl_n(K)$ définit un morphisme de groupes injectif.
  Pour tout groupe fini G, on a ainsi un morphisme de groupes injectif de G vers $Gl_{Card(G)}(K)$.
- Pro : Pour $K = \mathbb{F}_p$, le sous-groupe $UT_n(\mathbb{F}_p)$ des matrices triangulaires supérieures avec des 1 sur la diagonale est de cardinal $p^{\frac{n(n-1)}{2}}$.
  C'est donc un p-Sylow de $Gl_n(\mathbb{F}_p)$.
- App : Premier théorème de Sylow : Pour G groupe fini de cardinal n et pour tout p premier tel que $p|n$, G possède un p-Sylow.

2. Orbites et cycles. —

- Def : On définit le support de σ par $Supp(\sigma) := \{1,..,n\} - (\{1,..,n\}^\sigma)$.
- Pro : Deux permutations à support disjoint commutent.
- Def+Pro : Une transposition est une permutation σ dont le support possède exactement deux éléments $\{i,j\}$. On la note alors $\sigma := (i,j)$ car a $\sigma(i) = j$,$\sigma(j) = i$.
  Pour tout $2 \leq k \leq n$, un k-cycle est une permutation σ dont le support est de cardinal k et telle que $Supp(\sigma) = Orb_\sigma(i)$ pour un $i \in Supp(\sigma)$. On la note $\sigma := (i, \sigma(i), \sigma^2(i), .., \sigma^{k-1}(i))$. Pour tout $j \in Supp(\sigma)$, il existe $0 \leq l \leq k-1$ tq $j = \sigma^l(i)$.
  Un cycle c est un k-cycle pour un certain $2 \leq k \leq n$. On dit alors que c est de longueur k.
- Pro : Pour tout $n \geq 3$, le centre de Σ_n est réduit à $\{Id\}$.
  Par exemple, $(1,2)(1,2,3) = (2,3) \neq (1,2,3)(1,2) = (1,3)$.
- Pro : Pour tout $1 \leq k \leq n$, pour tous $i_1,..,i_k$ distincts, on a $(i_1, i_2, .., i_k) = (i_1, i_2)...(i_{k-1}, i_k)$.
- Pro : L'ensemble des k-cycles de Σ_n est de cardinal $\binom{n}{k}.(k-1)! = \frac{n.(n-1)..(n-k+1)}{k}$.
- Thm : Toute permutation $\sigma \in \Sigma_n$ se décompose en produit de cycles $c_1,..,c_r$ à support disjoint. On a alors $Supp(\sigma) = \bigcup_i Supp(c_i)$.
  De plus, cette décomposition est unique à l'ordre près.
- Def : On appelle type de $\sigma \in \Sigma_n$ la liste $l_1,..,l_s$ des cardinaux des orbites de σ sur $\{1,..,n\}$, rangés dans l'ordre croissant.
- Pro : Les $l_i \neq 1$ du type de σ sont les longueurs des cycles $c_1,..,c_r$ de la décomposition de σ en produit de cycles à supports disjoints.
- Ex : $\sigma = (1,4,5)(2,3) \in \Sigma_6$ est de type $[1,2,3]$.
- Pro : Le type $(l_1,..,l_s)$ de tout $\sigma \in \Sigma_n$ vérifie : $l_1 + .. + l_s = n$.
  Réciproquement, tout s-uplet $(m_1,..,m_s) \in (\mathbb{N}^*)^s$ tel que $l_1 + .. + l_s = n$ est le type d'une permutation $\sigma \in \Sigma_n$.
- Pro : Pour $\sigma \in \Sigma_n$ de type $(l_1,..,l_s)$, $ord(\sigma) = ppcm(l_1,..,l_s)$.
- Ex : Ainsi, $\sigma = (1,3)(2,4,7,6,5) \in \Sigma_7$ est d'ordre 10.

3. Signature et groupe alterné. —

- Def+Pro : On définit l'application signature sur Σ_n par :
  $\varepsilon : \sigma \in \Sigma_n \mapsto \begin{cases} 1 \text{ si } \sigma \text{ est un produit de carrés} \\ -1 \text{ sinon} \end{cases}$.
  ε est un morphisme de groupes de Σ_n vers $\{-1,1\}$, de noyau l'ensemble des produits de carrés de permutations.
- Def : On appelle n-ième groupe alterné A_n le sous-groupe des éléments de Σ_n qui sont des produits de carrés.
- Rem : A_n est un sous-groupe distingué de Σ_n.
- Pro : On a $\varepsilon((i,j)) = -1$.
  Ainsi, pour tout $n \geq 2$, A_n est un sous-groupe strict de Σ_n, de cardinal $\frac{n!}{2}$.
- Pour $n = 2$, $A_2 = \{Id\}$. Pour $n = 3$, $A_3 = \{Id, (1,2,3), (1,3,2)\} \simeq \mathbb{Z}/3\mathbb{Z}$.
- Ex : Liste des 12 éléments de A_4.
- Cor : Pour $\sigma = c_1..c_r$, avec c_i de longueur m_i, on a $\varepsilon(\sigma) = \Pi_i(-1)^{m_i}$.
- Pro : On a aussi : $\varepsilon(\sigma) = \Pi_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$
- Pro : Pour tout $n \geq 3$, A_n est $(n-2)$-transitif.

2. Structure de Σ_n et A_n. —

1. Classes de conjugaison. —

- Pro : Soit $c = (i_1,..,i_k)$ un k-cycle et $\sigma \in \Sigma_n$.
  On a $\sigma.c.\sigma^{-1} = (\sigma(i_1),..,\sigma(i_k))$.
- Cor : La conjugaison préserve le type.
- Cor : Pour tout $n \geq 4$, le centre de A_n est trivial.

- Pro : Les 3-cycles sont tous conjugués.
  Les doubles-transpositions $(i,j)(k,l)$ sont toutes conjuguées.
- Pro : Deux permutations de Σ_n sont congruentes ssi elles ont le même type.
- Rem : Les classes de conjugaison de Σ_n sont ainsi représentées par le type de l'un de leurs éléments.
- **Dev** : Théorème de Brauer : Soit $\mathbb{K}$ un corps de caractéristique quelconque, $n \geq 1$, et $\sigma, \sigma' \in \Sigma_n$.
  Alors σ et σ' sont conjuguées si et seulement si leurs matrices de permutation $T_\sigma, T_{\sigma'}$ sont semblables dans $Gl_n(\mathbb{K})$.

2. Générateurs. —

- Thm : Soit $n \geq 2$. On a :
  i) Les transpositions engendrent Σ_n.
  ii) Les transpositions $(1,i)$, $\forall 2 \geq i \geq n$ engendrent Σ_n.
  iii) Les transpositions $(i,i+1)$, $\forall 1 \geq i \geq n-1$ engendrent Σ_n.
  iv) Les permutations $(1,2)$ et $(1,2,..,n)$ engendrent Σ_n.
- Ex : $(k,k+1) = (1,2,..,n)^{k-1}.(1,2).(1,2,..,n)^{-(k-1)}$.
  $(k,k+1) = (1,k)(1,k+1)(1,k)$.
  Pour $i<j$, $(i,j) = ((i,i+1)(i+1,i+2)..(j-2,j-1))(j-1,j).((j-2,j-1)..(i,i+1))$.
- Cor : Pour $n \geq 3$, A_n est engendré par les 3-cycles (i,j,k).
- Ex : Pour $n \geq 4$, $(1,2)(3,4) = (1,2,3)(2,3,4)$.
- **Dev** : Pour tout $n \geq 5$, le groupe alterné A_n est simple.
- Contre-ex : Le sous-groupe V_4 des doubles-transpositions de Σ_4 est distingué dans A_4.
- Pro : Pour $n \geq 5$, le groupe dérivé de Σ_n est A_n, et le groupe dérivé de A_n et A_n.
- Pro : Sous-groupes distingués de Σ_n.
- Thm : Les sous-groupes de Σ_n d'indice n sont isomorphes à Σ_{n-1}.

3. Applications. —

On se donne K un corps et un $n \geq 1$. A est un anneau commutatif unitaire.

1. Déterminant. —

- Définition du déterminant d'une matrice de taille $n \times n$.
- Pro : det est n-linéaire et alterné.
- Pro : det est invariant par permutation des colonnes ou des lignes.
- Pro : $det((a_{i,j})_{i,j}) = \Pi_{\sigma \in \Sigma_n} \varepsilon(\sigma) a_{1,\sigma(1)}..a_{n,\sigma(n)}$.
- Ex : $det(\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$.
- Ex : $det(A)$ pour n=3.
- Thm : det est l'unique forme n-linéaire alternée valant 1 sur une base donnée.
- Pro : $det(A^t) = det(A)$.
- Thm : Une matrice de $M_n(K)$ est inversible ssi elle envoie la base canonique de K^n sur une base, ssi $det(A) \in K^*$.
- App : Pour $a_1,..,a_n \in K$, on note $V_n(a_1,..,a_n)$ le déterminant de la matrice de Vandermonde des a_i.
  On a $V_n(a_1,..,a_n) = \Pi_{i<j}(a_i - a_j)$.
  La matrice de Vandermonde est donc inversible ssi les a_i sont tous distincts.

2. Polynômes symétriques, alternés. —

- Def+Pro : On peut faire agir Σ_n sur $A[X_1,..,X_n]$ par $\sigma.P(X_1,..,X_n) = P(X_{\sigma(1)},..,X_{\sigma(n)})$.
  Pour tout $\sigma \in \Sigma_n$, $P \mapsto \sigma.P$ est un isomorphisme d'anneaux.
  On appelle polynômes symétriques les éléments de $A[X_1,..,X_n]^{\Sigma_n}$.
- Ex : $P = XY + YZ + ZY$ est un polynôme symétrique de $\mathbb{Z}[X,Y,Z]$.
- Def+Pro : Pour $1 \leq k \leq n$, on définit $\Sigma_k(X_1,..,X_n) := \sum_{1 \leq i_1 < .. < i_k \leq n} X_{i_1}..X_{i_k}$.
  Ces polynômes sont symétriques, et sont appelés polynômes symétriques élémentaires.
- Ex : Pour n=2, $\Sigma_0 = 1$, $\Sigma_1 = X_1 + X_2$, $\Sigma_2 = X_1 X_2$.
- Ex : Le déterminant de Vandermonde $V_n(X_1,..,X_n)$ n'est pas un polynôme symétrique si $car(K) \neq 2$, mais V_n^2 si.
- Thm : Relations coefficients-racines : Soit $P \in A[X]$ et $(\alpha_1,..,\alpha_n)$. On a l'équivalence :
  i) $P(X) = (X - \alpha_1)..(X - \alpha_n)$.
  ii) $P(X) = X^n + a_{n-1}X^{n-1} + .. + a_0$ avec $a_{n-i} = (-1)^i \Sigma_i(\alpha_1,..,\alpha_n)$.
- Théorème de structure des polynômes symétriques : L'application $P \mapsto P(\Sigma_1,..,\Sigma_n)$ est un isomorphisme d'anneaux A-linéaire entre $A[X_1,..,X_n]$ et $A[X_1,..,X_n]^{\Sigma_n}$.
  Ainsi, tout polynôme symétrique est un polynôme en les polynômes symétriques élémentaires.
- Algorithme de factorisation d'un polynôme symétrique : Entrées : P. Sortie : S tel que $P(\Sigma_1,..,\Sigma_n) = P$. Initialisation : S=0.
  Pour P polynôme symétrique, tant que le monôme de plus haut degré pour l'ordre lexicographique n'est pas constant, regarder le monôme $X_1^{a_1}..X_n^{a_n}$, poser Q=$X_1^{a_1-a_2}.X_2^{a_2-a_3}..X_{n-1}^{a_{n-1}-a_n}.X_n^{a_n}$, poser S=S+Q, et $P = P - Q(\Sigma_1,..,\Sigma_n)$.
  Lorsque P est constant, renvoyer $S + P(0)$.
- Def : Comme A_n est un sous-groupe de Σ_n, on peut aussi définir l'ensemble des polynômes alternés $A[X_1,..,X_n]^{A_n}$
- Pro : Soit P un polynôme alterné. Pour tous σ, τ tq $\varepsilon(\sigma) = \varepsilon(\tau)$, on a $\sigma.P = \tau.P$.
- Thm : Soit A intègre. Pour $U_n = \Pi_{i<j}(X_i + X_j)$, le polynôme $W_n := \frac{V_n + U_n}{2}$ est à coefficients entiers, et tout polynôme $P \in A[X_1,..,X_n]$ alterné s'écrit $P = Q + W_n.R$ avec Q,R symétriques.
- Rem : Si 2 est inversible dans A, on peut remplacer W_n par V_n et obtenir rapidement la décomposition souhaitée en écrivant $P = \frac{P+\tau.P}{2} + \frac{P-\tau.P}{2}$ pour τ de signature -1.
- Pro : Formules de Newton : En posant $S_k(X_1,..,X_n) = X_1^k + .. + X_n^k$, on a :
  i)$\forall 1 \leq k \leq n$, $S_k - \Sigma_1.S_{k-1} + .. + (-1)^{k-1}\Sigma_{k-1}.S_1 + (-1)^k k\Sigma_k = 0$.
  ii) $\forall k \geq n$, $S_k - \Sigma_1.S_{k-1} + .. + (-1)^{k-1}\Sigma_{k-1}.S_1 + (-1)^n S_{k-n}\Sigma_n = 0$
- App : Caractérisation des matrices nilpotentes : Soit $A \in M_n(\mathbb{K})$. A est nilpotente sse $\forall 1 \leq k \leq n$, $Tr(A^k) = 0$.

Références

Ulmer : Permutation, cardinalié, structure de groupe, notation, morphisme structurel, Th de Cayley, matrices de permutation. Support d'une permutation, k-cycles, décomposition en cycles à supports disjoints, type, ordre en fonction du type, exemples. Signature, groupe alterné, signature d'une transposition, propriétés. Classes de conjugaison, 3-cycles, doubles-transposition, préservation du type. Générateurs de Σ_n.

Perrin : Application au premier th de Sylow. Contre-ex V_4, groupes dérivés, sous-groupes distingués, propriétés.

Gourdon : Déterminant, définition, propriétés, exemples. Polynômes symétriques.

Ramis, Deschamps, Odoux : Polynômes symétriques, propriétés, Th de structure, algorithme de factorisation.

FGN : Formules de Newton.

Lang : A_n est simple.(Dev)

Sans Ref : Th de Brauer.(Dev), Th de structure des polynômes alternés.

January 23, 2018

Vidal Agniel, École normale supérieure de Rennes