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

[BER] p. 199 - 210

I) Le groupe symétrique

A) Définitions - premières propriétés

On note E un ensemble fini à n éléments, $n \geq 1$.

Déf 1 : L'ensemble des bijections de E sur lui-même est un groupe pour la composition d'applications, appelé groupe des permutations de E, ou groupe symétrique de E, noté S_E ou $\mathfrak{S}_E$. Un élément de S_E est appelé permutation.

Rem 2 : $|S_E| = n!$

Ex 3 : Si $E = [\![1;n]\!]$, et $\sigma \in S_E$, on note $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.
Par exemple : $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 2$.

Lemme 4 : Si E et E' sont deux ensembles non vides en bijection, alors $\mathfrak{S}_E \simeq \mathfrak{S}_{E'}$ (valable aussi si E, E' infinis)

Rem 5 : Grâce à ce lemme, dans la suite on étudie $S_n := S_{[\![1;n]\!]}$. $(E = [\![1;n]\!])$.
Tous les résultats sont valables sur $\mathfrak{S}_E$ grâce à l'isomorphisme.

THM 6 : (De Cayley) Si G est un groupe fini d'ordre n, alors il est isomorphe à un sous-groupe de S_n.

Déf 7 : Soit $\sigma \in S_n$, son support est : $\mathrm{supp}(\sigma) = \{a \in E \mid \sigma(a) \neq a\}$.

Prop 8 : Pour tout $\sigma \in S_n$, on a : (1) $\sigma(\mathrm{Supp}(\sigma)) = \mathrm{Supp}(\sigma)$
(2) $\mathrm{supp}(\sigma) = \mathrm{supp}(\sigma^{-1})$; (3) $\forall m \in \mathbb{Z}$, $\mathrm{supp}(\sigma^m) \subseteq \mathrm{supp}(\sigma)$
(4) $\forall \sigma' \in S_n$, $\mathrm{supp}(\sigma\sigma') \subseteq \mathrm{supp}(\sigma) \cup \mathrm{supp}(\sigma')$ avec égalité si les supports sont disjoints.

Prop 9 : Deux permutations à supports disjoints commutent.

Déf 10 : Pour $\sigma \in S_n$ et $a \in E$, la σ-orbite de a est : $\mathrm{Orb}_\sigma(a) = \{\sigma^m(a) \mid m \in \mathbb{Z}\}$.

Rem 11 : Les σ-orbites de E forment une partition de E. Si $|\mathrm{Orb}_\sigma(a)| = p$, p est le plus petit entier strictement positif tel que $\sigma^p(a) = a$.

Déf 12 : $\sigma \in S_n$ est un cycle lorsqu'il n'existe qu'une seule σ-orbite non réduite à un singleton. Si $p \geq 2$ est le cardinal de cette orbite, on dit que σ est un p-cycle. Un 2-cycle est appelé transposition.

Ex 13 : $p \geq 2$, $\{a_1, \dots, a_p\} \subseteq E$, $\sigma \in S_n$ définie par $\begin{cases} \sigma(a_i) = a_{i+1} \ \forall i \in [\![1;p-1]\!] \\ \sigma(a_p) = a_1, \ \sigma(x) = x, \ \forall x \notin \{a_1, \dots, a_p\} \end{cases}$
est un p-cycle. On le note $\sigma = (a_1\, a_2 \dots a_p)$
$\tilde{\sigma} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (1\,3\,2) = (3\,2\,1) = (2\,1\,3)$.

Prop 14 : Soit $p \geq 2$, pour tout $\sigma \in S_n$, p-cycle, il existe $a \in E$ tel que $\sigma = (a\ \sigma(a)\ \sigma^2(a) \dots \sigma^{p-1}(a))$.

B) Générateurs - classes de conjugaison

THM 15 : Soit $\sigma \in S_n$, σ se décompose en produit de cycles à supports disjoints, et cette décomposition est unique à l'ordre des facteurs près.
On a $\sigma = \prod_{\omega \in \Omega^*} \sigma_\omega$, où Ω^* = ensemble des σ-orbites non réduites à un point et $\sigma_\omega = (a, \sigma(a) \dots \sigma^{|\omega|-1}(a))$, $a \in \omega$

Ex 16 : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix} = (1\,5)(2\,6\,3)$.

Cor 17 : S_n est engendré par les cycles.

THM 18 : S_n est engendré par les transpositions.

Cor 19 : L'ordre d'une permutation est le ppcm des longueurs des cycles à supports disjoints qui la composent.

Prop 20 : Soit $\tau \in S_n$. Pour tout $\sigma = (a_1, \dots, a_p)$ p-cycle, $\tau\sigma\tau^{-1} = (\tau(a_1)\, \tau(a_2) \dots \tau(a_p))$.

THM 21 : Deux permutations sont conjuguées dans S_n si, et seulement si, leur liste (avec répétition) des longueurs des cycles à supports disjoints qui les composent sont les mêmes à l'ordre près.

Ex 22 : $\sigma = (1\,3\,5)(2\,4)$ et $\sigma' = (1\,2\,3)(6\,7)$ sont conjuguées dans S_7 via $\tau = (2\,6\,4\,7\,5\,3)$.

Prop 23 : S_n est engendré par :
- les transpositions $(1,i)$, $\forall i \in [\![2;n]\!]$
- $(1\,2)$ et $(1\,2 \dots n)$
- les transpositions $(i,i+1)$, $\forall i \in [\![1;n-1]\!]$

~~Prop 24~~

[BER] p. 204 - 210 - [BER] p. 212 - 213

II) Le groupe alterné A_n

A) Le morphisme signature : $n \geq 2$.

THM-Déf 24 : Il existe un unique morphisme $\varepsilon : S_n \to \mathbb{C}^\times$ non trivial. Si $\sigma \in S_n$ s'écrit comme produit de s transpositions, on a : $\varepsilon(\sigma) = (-1)^s$. ε est appelé morphisme signature.

Rem 25 : Le théorème précédent donne implicitement le résultat suivant : La parité du nombre de transpositions nécessaire pour écrire une permutation ne dépend pas de la décomposition choisie.

Ex 26 : $\varepsilon(\mathrm{id}) = 1$, pour σ un p-cycle, $\varepsilon(\sigma) = (-1)^{p-1}$

Prop 27 : Pour $\sigma \in S_n$, $\varepsilon(\sigma) = (-1)^{n - N_\sigma}$ où N_σ est le nombre de σ-orbites (même réduite à un point)

THM 28 : $\forall \sigma \in S_n$, $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$

Rem 29 : On en déduit que $\varepsilon(\sigma) = (-1)^{\nu(\sigma)}$ où $\nu(\sigma) = \left| \{(i,j) \in [\![1;n]\!]^2 \mid i < j \text{ et } \sigma(j) < \sigma(i)\} \right|$

[BER] p. 213 - 214 - [FGN] p. 50

B) Structure de $\mathfrak{A}_n$

[ROM] p.51 – 52

Déf 30 : On dit qu'une permutation $\sigma \in \mathfrak{S}_n$ est paire (respectivement impaire) lorsque $\varepsilon(\sigma) = 1$ (resp. $\varepsilon(\sigma) = -1$)
- Le groupe alterné est le sous-ensemble formé des permutations paires. On le note $\mathfrak{A}_n$.

Rem 31 : En tant que noyau du morphisme ε, on a $\mathfrak{A}_n \triangleleft \mathfrak{S}_n$ et $|\mathfrak{A}_n| = \frac{n!}{2}$.
- $\mathfrak{A}_2 = \{id\}$, $\mathfrak{A}_3$ est cyclique engendré par $(1\,2\,3)$.

THM 32 : $\forall n \geq 3$, $\mathfrak{A}_n$ est engendré par les 3-cycles.

Lemme 33 : Soit $n \geq 3$ et $k \leq n-2$. Soit $\{a_1, \dots, a_k\} \subseteq [\![1, n]\!]$, $\{b_1, \dots, b_k\} \subseteq [\![1, n]\!]$,
$\exists \sigma \in \mathfrak{A}_n$ tq : $\forall i \in [\![1, k]\!]$, $\sigma(a_i) = b_i$.

[PER]

THM 34 : $\forall n \geq 5$, $\mathfrak{A}_n$ simple (Dév. 1)

[BER] p.219 – 220

Rem 35 : - Ce résultat dû à [illegible] est important car il permet de démontrer l'impossibilité de résoudre par radicaux une équation polynomiale de degré $n \geq 5$.
- $n = 3$, $\mathfrak{A}_3$ cyclique d'ordre 3, est simple
- $n = 4$, $H = \{id, (12)(34); (13)(24); (23)(14)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est distingué dans $\mathfrak{A}_4$ (c'est même son groupe dérivé). Donc $\mathfrak{A}_4$ n'est pas simple.

Lemme 36 : $n \geq 3$, $Z(\mathfrak{S}_n) = \{id\}$; $n \geq 4$, $Z(\mathfrak{A}_n) = \{id\}$.

Cor 37 : Soit $n \geq 2$, $n \neq 4$. Les sous-groupes distingués de $\mathfrak{S}_n$ sont : $\{id\}$; $\mathfrak{A}_n$; $\mathfrak{S}_n$; et $[D(\mathfrak{S}_n) = D(\mathfrak{A}_n) = \mathfrak{A}_n$ pour $n \geq 5]$

[PER] 19 – 21

Prop 38 : Soit H un sous-groupe d'indice n de $\mathfrak{S}_n$, alors $H \simeq \mathfrak{S}_{n-1}$.

THM 39 : Pour $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur : $Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$
c-à-d : $\forall \varphi \in Aut(\mathfrak{S}_n)$, $\exists g \in \mathfrak{S}_n$ tq $\varphi = i_g : x \mapsto gxg^{-1}$.

Rem 40 : Pour $n = 6$, ~~le résultat~~ on peut montrer que le résultat devient faux.

25

III) Applications :

A) Déterminant : K un corps commutatif, E un K-e.v. $n \in \mathbb{N}^*$

[BER] p.62 – 69

Déf 41 : $\varphi : E^n \to K$ est une forme n-linéaire antisymétrique lorsque : $\forall (x_1, \dots, x_n) \in E^n$, $\forall \sigma \in \mathfrak{S}_n$, $\varphi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma)\varphi(x_1, \dots, x_n)$
- On dit qu'elle est ~~anti~~ alternée lorsque : $\forall (x_1, \dots, x_n) \in E^n$, $x_i = x_j$ pour $i \neq j$ implique $\varphi(x_1, \dots, x_n) = 0$.

Prop 42 : Si $car(K) \neq 2$, une forme n-linéaire est alternée si et seulement si elle est antisymétrique.

THM-Déf 43 : On suppose E de dimension $n \geq 1$. Le K-espace vectoriel $Alt_n(E)$ des formes n-linéaires alternées est de dimension 1.
- Pour toute base $e = (e_1, \dots, e_n)$ de E, il existe une unique forme n-linéaire alternée $\det_e$ telle que $\det_e(e_1, \dots, e_n) = 1$. $\det_e$ engendre $Alt_n(E)$.
Et si $x_j = \sum_{i=1}^{n} a_{ij} e_i$, $\det_e(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1)1} \times \dots \times a_{\sigma(n),n}$. Cette quantité est le déterminant de $x_1, \dots, x_n$ par rapport à la base e.

Prop 44 : Avec les notations précédentes. On a
$\det_e(x_1, \dots, x_n) \neq 0 \iff (x_1, \dots, x_n)$ libre $\iff (x_1, \dots, x_n)$ base de E

Déf 45 : - Pour $u \in \mathcal{L}(E)$, son déterminant est : $\det(u) = \det_e(u(e_1), \dots, u(e_n))$ où $e = (e_1, \dots, e_n)$ base arbitraire de E. Ce déterminant est indépendant de la base choisie
- Pour $M \in M_n(K)$, son déterminant est le déterminant des ses vecteurs colonnes dans la base canonique de K^n. C'est aussi le déterminant de l'endomorphisme $\left| \begin{array}{l} K^n \to K^n \\ X \mapsto MX \end{array} \right.$. Donc si $M = (a_{ij})$, $\det(M) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i)i}$.

Prop 46 : $M \in M_n(K)$, $\det(M) = \det({}^tM)$

[BEC]

Lemme 1 : $p \geq 3$ premier. L'unique morphisme non trivial de $\mathbb{F}_p^\times \to \{\pm 1\}$ est $L = \left(\frac{\circ}{p}\right)$, symbole de Legendre.

Lemme 2 : $D(GL_n(\mathbb{F}_p)) = SL_n(\mathbb{F}_p)$ ($p \geq 3$ premier)

THM 47 : (Frobenius-Zolotarev) : $p \geq 3$, premier. $\forall u \in GL_n(\mathbb{F}_p)$, $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$ (Dév 2)

B) Matrices de permutation :

[ROM] p.56

Déf 48 : Pour $\sigma \in \mathfrak{S}_n$, on lui associe la matrice de passage P_σ de la base canonique $\mathcal{B} = (e_j)_{j=1}^n$ de K^n à la base $\mathcal{B}_\sigma = (e_{\sigma(j)})_{j=1}^n$. On appelle P_σ matrice de permutation associée à σ.

Rem 49 : Pour un vecteur $x = (x_j)_{j=1}^n \in K^n$, on a $P_\sigma x = (x_{\sigma^{-1}(j)})_{j=1}^n$

III) B)

[RAN] p°56

THM 50 : L'application $\left|\begin{array}{ccc} S_n & \longrightarrow & GL_n(K) \\ \sigma & \longmapsto & P_\sigma \end{array}\right.$ est un morphisme de groupe injectif.
Et on a : $\forall \sigma \in S_n$, $\det(P_\sigma) = \varepsilon(\sigma).1_K$.

Appli 51 : Tout sous-groupe fini d'ordre $n \geq 1$ est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p)$, où $p \geq 2$ premier.

[BEC] p°321

THM 52 (Brauer) : Soit $\sigma, \tau \in S_n$.
σ, τ conjuguées dans $S_n \iff P_\sigma, P_\tau$ semblables dans $GL_n(K)$

(peut être un développement)

- Pas dire que historiquement c'est dû à Abel
- Dire que la théorie des grpe apparaît avec S_n
  ↳ étude des permutat° de racines de polyn. par ex
- Manque S_3, A_4, S_4 comme grpe des isométries de trucs...

C) Polynômes symétriques :

On note A un anneau intègre

[ROM] p°57

Déf 53 : Un polynôme $P \in A[X_1, \dots, X_n]$ est dit symétrique lorsque :
$P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$, $\forall \sigma \in S_n$.

Ex 54 : $\forall k \in [\![1; n]\!]$, $\Sigma_{k,n} = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} X_{i_2} \dots X_{i_k} = \sum_{\substack{I \subseteq [\![1,n]\!] \\ |I| = k}} \left(\prod_{j \in I} X_j \right)$ sont des polynômes symétriques. On les appelle polynômes symétriques élémentaires.

♥ ou [GOZ]

THM 55 : (Relations coefficients-racines) Soit $P \in K[X]$ (K algébriquement clos) de degré $n \geq 1$ unitaire, de racines $x_1, \dots, x_n$ (comptées avec multiplicité)
On note : $\forall i \in [\![1; n]\!]$, $\sigma_i = \Sigma_{i,n}(x_1, \dots, x_n)$. Alors :

$$P = X^n + \sum_{i=1}^{n} (-1)^i \sigma_i X^{n-i}$$

Ex 56 : Pour $P = (X-a)(X-b)(X-c)$, $P = X^3 - \underbrace{(a+b+c)}_{\sigma_1} X^2 + \underbrace{(ab+ac+bc)}_{\sigma_2} X - \underbrace{abc}_{\sigma_3}$.

[RAN]

THM 57 : Soit $P \in A[X_1, \dots, X_n]$ symétrique, alors il existe un unique polynôme $Q \in A[X_1, \dots, X_n]$ tel que : $P(X_1, \dots, X_n) = Q(\Sigma_{1,n}, \dots, \Sigma_{n,n})$.

Ex 58 : $X_1^2 + X_2^2 + X_3^2 = \Sigma_{1,3}^2 - 2\Sigma_{2,3}$

Appli 50 : (Théorème de Kronecker) Soit $P \in \mathbb{Z}[X]$, de degré $n \geq 1$ tel que $P(0) \neq 0$, de racines complexes $z_1, \dots z_n$.
Si : $\forall i \in [\![1; n]\!]$, $|z_i| \leq 1$, alors ce sont des racines de l'unité.

[FRA]

Appli 51 : $\mathbb{C}$ est algébriquement clos.

[GOU]

Réf :
- [BER] - Berhuy, Algèbre : Le grand combat
- [ROM] - Rombaldi - Algèbre
- [PER] - Perrin

([FRA] Francinou Oraux Xens Algèbre 1
[GOZ] - Gozard ; [GOU] - Gourdon ; [BEC] Beck)

bosser représentat° de grpe

Dév. 1) A_n simple, $n \geq 5$ [PER]
2) Frobenius-Zolotarev ≃ [BEC]