Groupe Symétrique

I. Compléments sur les groupes

$\star$ Si $(G, *)$ est un groupe fini, son cardinal est appelé ordre de G.

$\star$ On a le théorème de Lagrange : si G est un groupe fini et si H est un sous-groupe de G alors, l'ordre de H divise l'ordre de G.

$\star$ Soient $(G, *)$ un groupe et A une partie de G. Le sous-groupe engendré par A, noté, $< A >$ est l'intersection de tous les sous-groupes de G qui contiennent A. On peut montrer que :

$$< A > = \Big\{ g \in G \ \ : \ \ \exists p \in \mathbb{N},\ \exists a_1, \cdots, a_p \in A,\ \exists \varepsilon_1, \cdots, \varepsilon_p \in \{-1, 1\},\ g = a_1^{\varepsilon_1} * \cdots * a_p^{\varepsilon_p} \Big\}$$

$\star$ Un groupe $(G, *)$ est dit monogène lorsqu'il existe $g \in G$ tel que $G = < g >$. L'élément g est alors appelé un générateur de G. Il n'y a pas unicité du générateur. On a :

$$G = \Big\{ g^n \ \ : \ \ n \in \mathbb{Z} \Big\}$$

Un tel groupe est toujours abélien.

$\star$ Un groupe monogène fini est dit cyclique.

$\star$ Soient $(G, *)$ un groupe et $g \in G$. On dit que g est d'ordre fini si il existe $k \in \mathbb{N}^*$ tel que $g^k = e_G$. On introduit alors l'ordre $\omega(g)$ de l'élément g définit comme :

$$\omega(g) = \inf_{\mathbb{N}^* \cup \{+\infty\}} \Big\{ k \in \mathbb{N}^* \ \ : \ \ g^k = e_G \Big\}$$

$\star$ Soit $(G, *)$ un groupe. Pour tous $g \in G$ et $m \in \mathbb{Z}$, on a les équivalences suivantes :

(i) $(g^m = e_G) \Leftrightarrow (\omega(g) \mid m)$

(ii) $(\ g \ \text{ est d'ordre fini } \ m\ ) \Leftrightarrow (\ < g > \ \text{ est d'ordre } \ m\ )$

Il en découle que tous les éléments de G ont un ordre qui divise celui de G.

$\star$ En particulier, un groupe dont l'ordre est un nombre premier est nécessairement cyclique : il est engendré par tous ses éléments sauf le neutre.

II. Groupe Symétrique

$\star$ Une permutation de $[1, n]$ est une bijection de $[1, n]$. On note $\mathcal{S}_n$ l'ensemble des permutations de $[1, n]$.

$\star$ On dit que $k \in [1, n]$ est fixe par $\sigma \in \mathcal{S}_n$ lorsque $\sigma(k) = k$. L'ensemble des entiers de $[1, n]$ qui ne sont pas fixes par σ est appelé le support de σ et est noté $\mathrm{supp}(\sigma)$.
Deux permutations à supports disjoints commutent.

$\star$ $(\mathcal{S}_n, \circ)$ est un groupe appelé le groupe symétrique d'indice n. Il est d'ordre $n!$. Il est non abélien dès que $n \geqslant 3$.

$\star$ On dit que $\sigma_1, \sigma_2 \in \mathcal{S}_n$ sont conjuguées lorsqu'il existe $\rho \in \mathcal{S}_n$ tel que :

$$\sigma_2 = \rho\, \sigma_1\, \rho^{-1}$$

La relation "être conjuguée à" est une relation d'équivalence. De plus l'application :

$$\varphi_\rho : \begin{cases} \mathcal{S}_n & \to & \mathcal{S}_n \\ \sigma & \to & \rho\, \sigma_1\, \rho^{-1} \end{cases}$$

est un automorphisme de groupe tel que $\varphi_\rho^{-1} = \varphi_{\rho^{-1}}$. On dit que c'est un automorphisme intérieur.

$\star$ Une transposition est une permutation qui échange deux éléments tout en laissant les autres fixes. Les transpositions sont des éléments d'ordre 2 de $\mathcal{S}_n$. Cependant, ce ne sont pas les seuls éléments d'ordre 2 !

$\star$ Toutes permutation est un produit de permutations à supports non nécessairement disjoints. Il n'y a pas unicité de cette décomposition.

Déterminants

Dans toute la suite, K est corps commutatif et E est un K-espace vectoriel de dimension finie. De plus, on prend $p \in \mathbb{N}^*$

I. Formes multilinéaires alternées

$\star$ Une application $f : E^p \to K$ à p variables est appelée une **forme p-linéaire** si elle est linéaire vis à vis de chacune de ses p variables. L'ensemble des formes p-linéaires sur E est noté $\mathcal{L}_p(E,K)$. C'est un K-espace vectoriel.
En particulier, on peut noter que si $f \in \mathcal{L}_p(E,K)$, on a :

$$f(\lambda_1 x_1, \cdots, \lambda_p x_p) = \lambda_1 \cdots \lambda_p f(x_1, \cdots, x_p) \text{ et } f(x_1, \cdots, 0_E, \cdots, x_p) = 0_K$$

$\star$ Une forme p-linéaire f est dite **alternée** si l'image par f de toute famille liée est 0_K. L'ensemble des formes p-linéaires alternées sur E est noté $\mathcal{A}_p(E,K)$.
Attention ! Une forme p-linéaire alternée peut très bien s'annuler sur une famille libre.

$\star$ On a la caractérisation des formes p-linéaires alternées suivante :

$$(f \in \mathcal{L}_p(E,K) \text{ est alternée}) \Leftrightarrow \big(f \text{ s'annule sur les familles redondantes}\big) \Leftrightarrow (f \text{ est antisymétrique})$$

$\star$ On peut en déduire les propriétés suivantes pour toute forme $f \in \mathcal{A}_p(E,K)$:

(i) $f(x_1, \cdots, x_p)$ n'est pas modifiée lorsqu'on ajoute à l'un des x_i une combinaison linéaire des autres ;

(ii) Pour toute permutation $\sigma \in \mathcal{S}_p$, on a :

$$f(x_{\sigma(1)}, \cdots, x_{\sigma(p)}) = \varepsilon(\sigma) f(x_1, \cdots, x_p).$$

$\star$ Si on pose $n = \dim E$, on a $\dim \mathcal{A}_n(E,K) = 1$. On sait de plus que $\mathcal{A}_n(E,K) = \mathrm{Vect}(\varphi)$ où φ est la forme n-linéaire non nulle suivante :

$$\varphi : \left(\sum_{i=1}^n a_{i,1} e_i \, , \cdots, \sum_{i=1}^n a_{i,n} e_i\right) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{k=1}^n a_{\sigma(k),k}$$

Plus généralement, pour tout $p \in \mathbb{N}^*$, on a : $\dim \mathcal{A}_p(E,K) = \begin{pmatrix} n \\ p \end{pmatrix}$.

II. Déterminants

$\star$ On appelle déterminant de la famille de vecteurs $\mathcal{F} = (\sum_{i=1}^n a_{i,1} e_i \, , \cdots, \sum_{i=1}^n a_{i,n} e_i)$ dans la base $\mathcal{B} = (e_1, \cdots, e_n)$ de E le scalaire :

$$\det_{\mathcal{B}}(\mathcal{F}) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{k=1}^n a_{\sigma(k),k}$$

C'est la seule forme n-linéaire alternée sur E telle que $\det_{\mathcal{B}}(\mathcal{B}) = 1$.

⋆ On a les formules suivantes :

(i) Si $f \in \mathcal{A}_p(E,K)$, on a $f = f(\mathcal{B}) \det_{\mathcal{B}}$;

(ii) Pour toutes bases $\mathcal{B}$ et $\mathcal{B}'$, on a $\det_{\mathcal{B}'}(\mathcal{F}) = \det_{\mathcal{B}'}(\mathcal{B}) \det_{\mathcal{B}}(\mathcal{F})$ (Formule de changement de base).

⋆ On a l'équivalence suivante :

$$\left(\det_{\mathcal{B}}(\mathcal{F}) \neq 0_K\right) \Leftrightarrow (\mathcal{F} \text{ est une base de } E)$$

⋆ On appelle déterminant d'un endomorphisme u de E le scalaire $\det(u) = \det_{\mathcal{B}}(u(\mathcal{B}))$. Il ne dépend pas de la base $\mathcal{B}$ choisie.

⋆ On a les propriétés suivantes pour le déterminant d'un endomorphisme :

(i) $\det_{\mathcal{B}}(u(\mathcal{F})) = \det(u) \det_{\mathcal{B}}(\mathcal{F})$;

(ii) $\det(uv) = \det(u)\det(v)$ donc $\det(uv) = \det(vu)$;

(iii) $(u \in \mathcal{GL}(E)) \Leftrightarrow (\det(u) \neq 0_K)$. Dans ce cas, on a $\det(u^{-1}) = (\det(u))^{-1}$.

⋆ det induit un morphisme de groupes entre $(\mathcal{GL}(E), \circ)$ et $(K^*, \times)$. Son noyau est appelé le groupe spécial linéaire et est noté $\mathcal{SL}(E)$:

$$\mathcal{SL}(E) = \{u \in \mathcal{GL}(E) \;:\; \det(u) = 1_K\}$$

⋆ Soit $A = (a_{i,j}) \in \mathcal{M}_n(K)$. On appelle déterminant de A le scalaire :

$$\det A = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{k=1}^{n} a_{\sigma(k),k}$$

On note :

$$\det(A) = \begin{vmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{vmatrix}$$

⋆ Le déterminant d'une matrice triangulaire est égal au produit des coefficients diagonaux. Donc une matrice triangulaire est inversible si, et seulement si, ses coefficients diagonaux sont tous non-nuls.

⋆ Toutes les propriétés des formes n-linéaires alternées se généralisent au déterminant d'une matrice en voyant celle-ci comme la famille constituée de ses colonnes.

⋆ On peut donner des liens entre les différents déterminants :

(i) Si A est la matrice de $\mathcal{F}$ dans la base $\mathcal{B}$, alors $\det_{\mathcal{B}}(\mathcal{F}) = \det(A)$;

(ii) Si A est ma matrice de u dans la base $\mathcal{B}$, alors $\det(u) = \det(A)$.

$\star$ Le déterminant d'une matrice est un invariant de similitude.

$\star$ det induit un morphisme de groupes entre $(\mathcal{GL}_n(K), \times)$ et $(K^*, \times)$. Son noyau est appelé le groupe spécial linéaire d'indice n et est noté $\mathcal{SL}_n(K)$:

$$\mathcal{SL}_n(K) = \{A \in \mathcal{GL}_n(K) \ : \ \det(A) = 1_K\}$$

$\star$ Le déterminant d'une matrice est multiplicatif ($\det(AB) = \det(A)\det(B)$) et une matrice est inversible si, et seulement si, son déterminant est non nul.

$\star$ On a $\det({}^tA) = \det(A)$. Autrement dit, le déterminant est une forme n-linéaire alternée aussi bien vis à vis des colonnes que des lignes de la matrice.

$\star$ On peut remarquer que le déterminant ne fait intervenir que des sommes et des produites de coefficients. Il a donc des propriétés polynomiales. **En particulier, si on peut définir la continuité sur le corps K, le déterminant est continu vis à vis de chacune de ses variables**.

$\star$ Le déterminant d'une matrice triangulaire par blocs est le produit des déterminants des blocs diagonaux :

$$\left|\begin{array}{c|c} B & D \\ \hline \mathbb{O} & C \end{array}\right| = \det(B)\det(C)$$

où, $B \in \mathcal{M}_n(K)$, $C \in \mathcal{M}_p(K)$ et $D \in \mathcal{M}_{n,p}(K)$.

$\star$ Pour calculer un déterminant, on se ramène à une matrice triangulaire par la méthode du pivot de gauss sachant que :

(i) L'échange de deux ligne (ou de deux colonnes) change le signe du déterminant ;

(ii) La multiplication d'une ligne (ou d'une colonne) par λ multiplie le déterminant par λ ;

(iii) L'ajout à une ligne (ou à une colonne) d'une combinaison linéaire des autres ne modifie pas le déterminant.

$\star$ Soit $A = (a_{i,j}) \in \mathcal{M}_n(K)$. Pour $1 \leqslant i, j \leqslant n$ On appelle cofacteur du coefficient $a_{i,j}$ le scalaire :

$$A_{i,j} = (-1)^{i+j}\Delta_{i,j}$$

où $\Delta_{i,j}$ est le déterminant de la matrice A à laquelle on a retiré les lignes i et j. C'est le mineur de A de coordonnées (i, j).

$\star$ On peut développer le déterminant de $A = (a_{i,j}) \in \mathcal{M}_n(K)$ par rapport à :

(i) La i-ème ligne :

$$\det(A) = \sum_{i=1}^{n} a_{i,j} A_{i,j}$$

(ii) La j-ème colonne :

$$\det(A) = \sum_{j=1}^{n} a_{i,j} A_{i,j}.$$

⋆ Soient $x_0, \cdots, x_n \in K$. On appelle déterminant de Vandermonde le déterminant d'ordre $n+1$ suivant :

$$V(x_0, \cdots, x_n) = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_0 & x_1 & x_2 & \cdots & x_n \\ x_0^2 & x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ x_0^n & x_1^n & x_2^n & \cdots & x_n^n \end{vmatrix}$$

On montre que :

$$V(x_0, \cdots, x_n) = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)$$

On remarque que $V(x_0, \cdots, x_n)$ est non nul si, et seulement si les x_i sont deux à deux distincts.

⋆ On appelle comatrice de A, la matrice notée Com A de $\mathcal{M}_n(K)$ dont les coefficients sont les cofacteurs de A :

$$\text{Com } A = \begin{pmatrix} A_{1,1} & \cdots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{n,1} & \cdots & A_{n,n} \end{pmatrix}$$

On a alors la formule d'inversion suivante :

$$A({}^t\text{Com } A) = ({}^t\text{Com } A)A = \det(A) I_n$$

Si $\det(A) \neq 0$, A est inversible et on a la formule d'inversion suivante :

$$A^{-1} = \frac{1}{\det(A)} ({}^t\text{Com } A)$$

⋆ Deux bases $\mathcal{B}$ et $\mathcal{B}'$ d'un $\mathbb{R}$-espace vectoriel E sont de même orientation si $\det_{\mathcal{B}'}(\mathcal{B}) > 0$. La relation "avoir la même orientation" est une relation d'équivalence sur l'ensemble des bases de E. Cette relation induit deux classes d'équivalence. Orienter E c'est choisir une de ces deux classes dont les éléments seront appelées bases directes. Les bases de la deuxième classe sont appelées bases indirectes ou rétrogrades.

⋆ Soit E un $\mathbb{R}$-espace vectoriel et $\mathcal{B}$ une base de E. On dit qu'un endomorphisme u de E conserve l'orientation lorsque $\det(u) > 0$. Alors, $u(\mathcal{B})$ est une base de E de même orientation que $\mathcal{B}$. Dans le cas contraire, on dit qu'il change l'orientation. Dans ce cas, $u(\mathcal{B})$ est une base de E d'orientation contraire à $\mathcal{B}$.