Groupe opérant sur un ensemble. Exemples et applications.

101

Cadre : Soient G un groupe, e son élément neutre, H un sous-groupe de G et X un ensemble.

I - Définitions et premières propriétés

1 - Actions de groupe

déf 1 : On dit que G opère ou agit sur X si on s'est donné une application $G \times X \longrightarrow X$, $(g,x) \longmapsto g.x$ vérifiant : 1) $\forall g,g' \in G, \forall x \in X, g.(g'.x) = (gg').x$ 2) $\forall x \in X, e.x = x$

On dit aussi que X est un G-ensemble. Et on note $G \curvearrowright X$.

ex 2 : $\mathfrak{S}(X)$ opère sur X par la relation $\sigma.x = \sigma(x)$ pour tout $\sigma \in \mathfrak{S}(X)$ et pour tout $x \in X$.

rq 3 : Il revient au même de se donner un morphisme $\varphi : G \longrightarrow \mathfrak{S}(X)$, $g \longmapsto \varphi(g)(x) = g.x$. On dit que φ est le morphisme structurel de l'action de G sur X.

déf 4 : on dit que G opère sur X :
- fidèlement si $\varphi : G \longrightarrow \mathfrak{S}(X)$ est injectif
- transitivement si : $\forall x \in X, \forall y \in X, \exists g \in G, g.x = y$

rq 5 : $G/\ker\varphi$ opère fidèlement sur X

ex 6 : Soient E un espace vectoriel et $\mathbb{P}(E)$ l'ensemble des droites vectorielles de E. Alors $GL(E)$ opère fidèlement sur $\mathbb{P}(E)$.

ex 7 : le groupe D_n des isométries du plan conservant un polygone régulier à n côtés agit fidèlement et transitivement sur l'ensemble des sommets

déf/prop 8 : Soit $G \curvearrowright X$. la relation $\sim$ définie par : $x \sim y \Leftrightarrow \exists g \in G, y = g.x$ est une relation d'équivalence sur X dont les classes d'équivalence sont appelées orbites des éléments de X sous l'action de G et notées $(G.x)$ pour $x \in X$. Autrement dit, $X = \bigcup_{x \in X/\sim} (G.x)$.

rq 9 : G opère transitivement sur $(G.x)$.

ex 10 : les orbites de $\mathbb{R}^n$ sous l'action naturelle de $O_n(\mathbb{R})$ sont les sphères de centre l'origine.

app 11 : décomposition d'une permutation en produit de cycles à supports disjoints.

déf 12 : Soit $G \curvearrowright X$. On appelle stabilisateur de $x \in X$ dans G, le sous-groupe $G_x := \{g \in G \mid g.x = x\} \subset G$.

ex 13 : le stabilisateur de $x \in X = \{1, \dots n\}$ sous l'action de $\mathfrak{S}_n$ sur X est isomorphe à un sous-groupe de $\mathfrak{S}_{n-1}$.

déf 14 : l'action de G sur X est dite libre si : $\forall x \in X, G_x = \{e\}$

prop 15 : Soit $\varphi : G \longrightarrow \mathfrak{S}(X)$ une action de G sur X. Le noyau $\ker(\varphi)$ de φ est l'intersection des stabilisateurs G_x des éléments $x \in X$: $\ker(\varphi) = \bigcap_{x \in X} G_x$

rq 16 : libre $\Rightarrow$ fidèle

déf 17 : on dit que l'action de G sur X est k-fois transitive si pour tout couple de k-uplets d'éléments distincts $(x_1, \dots, x_k)$ et $(y_1, \dots y_k)$, il existe $g \in G$ tel que $g.x_i = y_i$ pour tout $1 \leq i \leq k$.

ex 18 : l'action du groupe A_n sur $\{1, \dots n\}$ est $n-2$ transitive.

2 - Action d'un groupe fini sur un ensemble fini

prop 19 : Soit $G \curvearrowright X$. L'application $G/G_x \longrightarrow G.x$, $\bar{g} \longmapsto g.x$ est une bijection.

cor 20 : Si G est fini, $|G.x| = \frac{|G|}{|G_x|}$

ex 21 : $\mathfrak{S}_n \curvearrowright X = \{1, \dots n\}$ on a, $\mathfrak{S}_n / \mathfrak{S}_{n-1} \simeq X$.

prop 22 : on suppose G et X finis. Si $X = \bigcup_{i=1}^{n} X_i$ est la partition de X en orbites sous l'action de G et si $x_i \in X_i$, alors : $|X| = \sum_{i=1}^{n} |X_i| = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|}$.

prop 23 (Formule de Burnside) on suppose G et X finis et on note $X^g = \{x \in X \mid g.x = x\}$. Alors $\sum_{g \in G} |X^g| = \sum_{x \in X} |G_x|$ et le nombre n d'orbites de X sous l'action de G est donné par : $n = \frac{1}{|G|} \sum_{g \in G} |X^g|$

prop 24 : Soient p premier, G un p-groupe, X un G-ensemble fini. Alors $|X^G| = |X| \ [p]$

II - Groupe agissant sur lui-même

1 - Action par translation

déf 25 : G agit sur lui-même ($X = G$) par translation à gauche via : $G \times G \longrightarrow G$, $(g,h) \longmapsto g.h = gh$

prop 26 : cette action est fidèle et transitive

app 27 (Théorème de Cayley) Tout groupe fini d'ordre $n \in \mathbb{N}$ est isomorphe à sous-groupe de $\mathfrak{S}_n$.

déf 28 : G agit sur l'ensemble des classes à gauche modulo H via $\varphi : G \times G/H \longrightarrow G/H$, $(g_1, g_2 H) \longmapsto g_1.(g_2 H) = (g_1 g_2)H$

prop 29 : c'est une action de groupe transitive dont le morphisme structurel est de la forme $\varphi : G \longrightarrow \mathfrak{S}_{(G:H)}$

rq 30 : cette action n'est pas fidèle en général ($\ker\varphi = \bigcap_{g \in G} gHg^{-1}$)

app 31 : Soient G un groupe infini et H un sous-groupe propre de G d'indice fini. Alors G n'est pas simple.

2 - Action par conjugaison

déf 32 : G opère sur lui-même par conjugaison via $\varphi : G \times G \to G$ $(g, h) \mapsto ghg^{-1}$

prop 33 : Pour $G \neq \{e\}$, cette action n'est pas libre, ni transitive.

déf 34 :
- L'orbite $\{ghg^{-1} / g \in G\}$ de $h \in G$ par l'action de conjugaison est appelée classe de conjugaison de h.
- deux éléments qui appartiennent à la même orbite sont dits conjugués
- le stabilisateur $Z_G(h) = \{g \in G / ghg^{-1} = h\}$ de h s'appelle centralisateur de h dans G.
- le stabilisateur d'un sous-groupe H de G est $N_G(H) = \{g \in G / gHg^{-1} = H\}$ On l'appelle le normalisateur de H dans G.

ex 35 : les stabilisateurs des éléments d'une même orbite sont conjugués

Rq 36 : le centre $Z(G)$ de G est l'ensemble des points fixes par conjugaison.

ex 37 :
- si n impair, les classes de conjugaison de D_n sont : $\{e\}$, $\{r^k, r^{-k}\}$ pour $k \in [\![1, \frac{n-1}{2}]\!]$ et $\{r^i s / i \in [\![1, n]\!]\}$ et $Z(D_n) = \{e\}$
- si n pair, les classes de conjugaison de D_n sont : $\{e\}$, $\{r^{\frac{n}{2}}\}$, $\{r^k, r^{-k}\}$ pour $k \in [\![1, \frac{n}{2} - 1]\!]$, $\{r^{2i} s / i \in [\![1, \frac{n}{2}]\!]\}$ et $\{r^{2i+1} s / i \in [\![1, \frac{n}{2}]\!]\}$ et $Z(D_n) = \{e, r^{\frac{n}{2}}\}$
- pour $n \geq 3$, $Z_{D_n}(r) = \langle r \rangle$

prop 38 : (Equation aux classes)
$|G| = |Z(G)| + \sum_i |\omega_i|$ où la somme porte sur toutes les classes de conjugaison de cardinal > 1

app° 39 : Soient p un nombre premier et G un p-groupe fini non trivial. Alors, le centre $Z(G)$ de G ne se réduit pas à $\{e\}$.

app° 40 : (Théorème de Cauchy)
Soit G un groupe fini d'ordre divisible par un nombre premier p. Alors, il existe dans G au moins un élément d'ordre p.

app° 41 : (Théorème de Wedderburn) **DEV 1**
Tout corps fini est commutatif.

prop 42 : i) si $\sigma \in \mathfrak{S}_n$ est un cycle d'ordre p, $\sigma = (a_1, \dots, a_p)$ et si $\tau \in \mathfrak{S}_n$, on a $\tau \sigma \tau^{-1} = (\tau(a_1), \dots, \tau(a_p))$
2) Dans $\mathfrak{S}_n$, tous les cycles d'ordre p sont conjugués
3) si $n \geq 5$, les cycles d'ordre 3 sont conjugués dans $\mathcal{A}_n$

lemme 43 : Soit $\sigma \in \mathcal{A}_n$. Notons $\mathcal{A}_n \cdot \sigma = \{\tau \sigma \tau^{-1} / \tau \in \mathcal{A}_n\}$ sa classe de conjugaison dans $\mathcal{A}_n$ et $\mathfrak{S}_n \cdot \sigma$ sa classe de conjugaison dans $\mathfrak{S}_n$.
→ S'il existe $\alpha \in \mathfrak{S}_n \setminus \mathcal{A}_n$ tel que $\alpha \sigma = \sigma \alpha$, alors $\mathcal{A}_n \cdot \sigma = \mathfrak{S}_n \cdot \sigma$ et $|\mathfrak{S}_n \cdot \sigma| = |\mathcal{A}_n \cdot \sigma|$
→ si pour tout $\alpha \in \mathfrak{S}_n \setminus \mathcal{A}_n$, $\alpha \sigma \neq \sigma \alpha$, alors $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathcal{A}_n}(\sigma)$ et $|\mathcal{A}_n \cdot \sigma| = \frac{1}{2} |\mathfrak{S}_n \cdot \sigma|$

app° 44 : $\mathcal{A}_n$ est simple $n \geq 5$

3 - Théorème de Sylow

déf 45 : Soient G un groupe fini de cardinal n et p un diviseur de n. Si $n = p^\alpha m$ avec $p \wedge m$, on appelle p-sous-groupe de Sylow de G un sous-groupe de cardinal p^α.

ex 46 : $P = \{A = (a_{ij}) / a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1\}$ est un p-Sylow de $GL_n(\mathbb{F}_p)$.

lemme 47 : Soit G un groupe avec $|G| = p^\alpha m$, $p \wedge m$ et soit H un sous-groupe de G. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

thm 48 : (Théorème de Sylow)
Soit G un groupe fini d'ordre $p^\alpha m$ avec $p \wedge m$. Alors :
1) G contient au moins un p-Sylow
2) si $H < G$ est un p-groupe, il existe un p-Sylow S de G tel que $H \subset S$
3) les p-Sylow sont tous conjugués
4) Soit n_p le nombre de p-Sylow de G, alors $n_p \equiv 1 \ (p)$ et n_p divise m

cor 49 : Soit S un p-Sylow de G. $S \lhd G \iff n_p = 1$

app 50 : un groupe d'ordre 63 n'est pas simple.

III. Applications en algèbre linéaire et en algèbre commutative.

Soit $\mathbb{K}$ un corps commutatif.

1 - Actions sur des espaces de matrices

déf 51 : $GL_n(\mathbb{K})$ agit par translation à gauche sur $\mathcal{M}_{n,p}(\mathbb{K})$ via : $P \cdot M \mapsto PM$.

prop 52 : Deux matrices de $\mathcal{M}_{n,p}(\mathbb{K})$ sont dans une même orbite ssi elles ont le même noyau.

app° 53 : Résolution de système linéaire

déf 54 : Soit E un espace vectoriel de dimension d. Pour $1 \leq r \leq d$, on pose $L_{r,d}$ l'ensemble des familles libres de vecteurs de E à r éléments. On dit que N respecte une famille $e = (e_1, \dots, e_r)$ de $L_{r,d}$ si, pour tout entier s compris entre 1 et r, on a $Ne_s = e_{s+1}$, on convient que $e_{r+1} = 0$.

prop 55 : l'action de $GL_d(\mathbb{F}_q)$ sur $L_{r,d}$ induit un morphisme : $GL_d(\mathbb{F}_q) \times L_{r,d} \to L_{r,d}$ où $L_{r,d}$ est vu comme l'ensemble $(P, M) \mapsto PM$ des matrices de $\mathcal{M}_{d,r}(\mathbb{K})$ de rang r.

app 56 (cône nilpotent) **DEV 2**
Pour tout corps fini $\mathbb{F}_q$ à q éléments et tout $d \in \mathbb{N}^*$, $|\mathcal{N}_d(\mathbb{F}_q)| = q^{d(d-1)}$ où $\mathcal{N}_d(\mathbb{F}_q)$ est l'ensemble des matrices nilpotentes de taille $d \times d$ à coefficients dans $\mathbb{F}_q$

prop57: le groupe $GL_m(\mathbb{K}) \times GL_n(\mathbb{K})$ agit sur $\mathcal{M}_{m,n}(\mathbb{K})$ via $(P,Q).M := PMQ^{-1}$

déf 58: Deux matrices de la même orbite pour cette action sont dites équivalentes

thm 59 (du rang): Deux matrices sont équivalentes ssi elles ont le même rang

app 60: si $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, $\overline{GL_n(\mathbb{K})} = \mathcal{M}_n(\mathbb{K})$

prop 61: $GL_n(\mathbb{K})$ agit sur l'espace des matrices symétriques $S_n(\mathbb{K})$ via l'action de congruence définie par: $\forall P \in GL_n(\mathbb{K}),\ \forall A \in S_n(\mathbb{K}),\ P.A = PA^tP$

déf 62: deux matrices symétriques A et A' de $S_n(\mathbb{K})$ sont dites congruentes si elles appartiennent à la même orbite pour cette action

thm 63: i) Si $\mathbb{K} = \mathbb{C}$, A et $A' \in S_n(\mathbb{C})$ sont dans la même orbite ssi elles ont même rang

2) Si $\mathbb{K} = \mathbb{R}$, A et $A' \in S_n(\mathbb{R})$ sont dans la même orbite ssi elles ont même signature $(p, n-p)$

3) Si $\mathbb{K} = \mathbb{F}_q$ est un corps de cardinal $q = p^\alpha$ avec $p \geq 3$ premier, deux matrices inversibles $A, A' \in S_n(\mathbb{F}_q)$ sont dans la même orbite ssi elles ont même discriminant.

app 64: loi de réciprocité quadratique

2. Actions sur un espace vectoriel: représentations linéaires des groupes finis

déf 65: on appelle représentation linéaire d'un groupe fini G, la donnée d'un espace vectoriel V et d'un morphisme de groupes $\rho_V : G \to GL(V)$, c'est donc une action de G sur V.
le degré de la représentation est la dimension de V

déf 66: le caractère χ_V de V est l'application $G \to \mathbb{C}$, $g \mapsto Tr(\rho_V(g))$.
On appelle degré de χ_V, l'entier $\chi_V(1) = \dim V$.

ex 67: - $\rho : G \to GL(V)$ est une représentation linéaire de G, appelée représentation $g \mapsto Id_V$ triviale, de caractère constant égal à 1.
- si X est un ensemble fini muni d'une action de G donnée par $(g,x) \mapsto g.x$, la représentation de permutation V_X est définie comme l'espace vectoriel V_X de dimension $|X|$, de base $(e_x)_{x \in X}$ muni d'une action linéaire de G: $g.e_x = e_{g.x}$ et $\chi_{V_X}(g) = |\{x \in X \mid g.x = x\}|$
- si on prend $X = G$ et l'action par translation, on obtient la représentation dite régulière V_G et $\chi_{V_G}(1) = |G|$, $\chi_{V_G}(g) = 0$ si $g \in G \setminus \{1\}$.
- Soient V_1, V_2 deux représentations de G et $u : V_1 \to V_2$ une application linéaire on définit la représentation $Hom(V_1, V_2)$ par $\rho_{Hom(V_1,V_2)}(g)(u) = \rho_{V_2}(g) \circ u \circ \rho_{V_1}(g^{-1})$ et $\chi_{Hom(V_1,V_2)}(g) = \overline{\chi_{V_1}(g)}\,\chi_{V_2}(g)$

app 68: table de $\mathfrak{S}_4$ (voir annexe)

3. Actions sur un espace de polynômes

Thm 69: (Théorème de Molien)
Soit G un groupe fini de $GL_n(\mathbb{C})$ qui agit linéairement sur le sous-groupe $V_d \subset \mathbb{C}[X_1, \dots X_n]$ des polynômes homogènes de degré d via: $\forall A \in G,\ \forall P \in V_d$, $A.P(X_1, \dots X_n) = P(A^{-1}(X_1, \dots X_n))$ qui revient à substituer $\sum_j a'_{ij} X_j$ à X_i si on note $A^{-1} = (a'_{ij})$. Alors: $\frac{1}{|G|} \sum_{A \in G} \frac{1}{\det(I - tA)} = \sum_{d \geq 0} \dim\left(V_d^G\right) t^d$.

Soit A un anneau commutatif unitaire.

prop 70: $\mathfrak{S}_n$ agit sur $A[X_1, \dots X_n]$ via σ. $P(X_1, \dots X_n) = P(X_{\sigma(1)}, \dots X_{\sigma(n)})$

déf 71: - on appelle ensemble des polynômes symétriques, l'ensemble des polynômes invariants sous l'action $\mathfrak{S}_n \curvearrowright A[X_1, \dots X_n]$ et on le note $A[X_1, \dots X_n]^{\mathfrak{S}_n}$
- les n polynômes Σ_p $(1 \leq p \leq n)$ définis par $\Sigma_p = \sum_{1 \leq i_1 < \dots < i_p \leq n} X_{i_1} \dots X_{i_p}$ sont appelés polynômes symétriques élémentaires.

ex 72: $\Sigma_1 = X_1 + X_2 + \dots + X_n$, $\Sigma_n = X_1 X_2 \dots X_n$

thm 73: (Théorème de structure des polynômes symétriques)
$$A[X_1, \dots X_n]^{\mathfrak{S}_n} = A[\Sigma_1, \dots \Sigma_n]$$

ex 74: Dans $A[X_1, X_2, X_3]$, $P = X_1^2X_2 + X_1^2X_3 + X_2X_1^2 + X_2^2X_3 + X_3X_1^2 + X_3^2X_2$ s'écrit $P = \Sigma_1\Sigma_2 - 3\Sigma_3$

IV. Application à la géométrie

1. Groupe projectif

Soit V un $\mathbb{K}$-ev de dimension finie $n \geq 2$.

prop 75: l'action naturelle de $GL(V)$ sur $\mathbb{P}(V)$ induit une action de $SL(V)$ sur $\mathbb{P}(V)$ et une action fidèle de $PSL(V)$ sur $\mathbb{P}(V)$ qui sont 2-transitives.
- Elle induit également une action fidèle et 3-transitive de $PGL(V)$ sur $\mathbb{P}(V)$

app 76:
- $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$
- $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$, $PSL_2(\mathbb{F}_3) \simeq \mathcal{A}_4$
- $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathcal{A}_5$

2. Espace affine

déf 77: On appelle espace affine, un ensemble $\mathcal{E}$ sur lequel le groupe additif $(E,+)$ d'un espace vectoriel agit à droite transitivement et librement via $\mathcal{E} \times E \to \mathcal{E}$, $(M, \vec{u}) \mapsto M + \vec{u}$. les éléments de $\mathcal{E}$ sont appelés les points et ceux de E les vecteurs

prop 78: l'action étant transitive et libre, pour tout couple de points (M,N) de $\mathcal{E}$, il existe un unique $\vec{x} \in E$ tel que $N = M + \vec{x}$.

ex 79: $SO(\mathbb{R}^2) \times (S^1 \times S^1) \to S^1 \times S^1$, $(r, (x,y)) \mapsto (r(x), r(y))$
l'orbite de (x,y) correspond à l'angle orienté des demi-droites $\mathbb{R}_x^+$ et $\mathbb{R}_y^+$

3. Groupes des isométries (dans $\mathbb{R}^3$)

déf/prop 80: Soient $\mathcal{E}$ un $\mathbb{R}$-espace affine de dimension 3 et X une partie non vide de $\mathcal{E}$. $O(E)$ désigne le groupe des isométries affines de $\mathcal{E}$. Le groupe $Isom(X) = \{f \in O(E) \mid f(X) = X\}$ (resp. $Isom^+(X) = \{f \in Isom(X) \mid \det f = 1\}$) des isométries (resp. positives) de l'ensemble X agit naturellement sur X.

prop 81: on note Δ_4 le tétraèdre régulier. $Isom(\Delta_4) \simeq \mathfrak{S}_4$ et $Isom^+(\Delta_4) \simeq \mathcal{A}_4$

prop 82: on note C_6 le cube en 3 dimensions. $Isom(C_6) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ et $Isom^+(C_6) \simeq \mathfrak{S}_4$

app 83: Vision géométrique de $\chi_{Hom(V_2, V_3)}$ dans la table de $\mathfrak{S}_4$

Annexe :

Table de $\mathfrak{S}_4$:

$\mathfrak{S}_4$	Id	(12)	(123)	(1234)	(12)(34)
χ_1	1	1	1	1	1
χ_ε	1	−1	1	−1	1
χ_5	3	1	0	−1	−1
$\chi_{\mathrm{Hom}(V_5, V_\varepsilon)}$	3	−1	0	1	−1
χ_5	2	0	−1	0	2

Références :

- Perrin, Cours d'algèbre
- Caldero-Germoni, H2G2
- Ulmer, Théorie des groupes
- RDO 1
- Combes
- Colmez
- Szpirglas

Développement: Théorème de Wedderburn

Adrien Fontaine

6 septembre 2013

Référence : Daniel Perrin, Cours d'algèbre, p82

Théorème 1

Tout corps fini est commutatif.

Démonstration : 1. Soit k un corps fini, a priori non nécéssairement commutatif, et Z le centre de k, *i.e*

$$Z = \{a \in k / \forall x \in k, ax = xa\}$$

Z est un sous-corps de k, commutatif, de cardinal $q \geq 2$ (il contient au moins 0 et 1). De plus, k est un Z-espace vectoriel, donc $|k| = q^n$.

2. On suppose par l'absurde que k est non commutatif, *i.e* $n \geq 2$. Alors, $k^\times$ opère de façon non triviale sur lui même par automorphisme intérieur. Pour $x \in k^\times$, on note $\omega(x)$ son orbite, *i.e*

$$\omega(x) = \{axa^{-1}, a \in k\}$$

On pose $k_x = \{y \in k, yx = xy\}$, l'ensemble des éléments qui commutent avec x. Alors, k_x est un sous-corps de k, et le stabilisateur de x sous l'action de $k^\times$ sur $k^\times$ est $k_x^\times$.
De plus, k_x est un Z-espace vectoriel, donc $|k_x| = q^d$. Et $k_x^\times$ est un sous-groupe de $k^\times$, donc $q^d - 1 \mid q^n - 1$. Écrivons la division euclidienne de n par d. Il existe $(q, r) \in \mathbb{N}^* \times \mathbb{N}$ tel que

$$n = dq + r \text{ et } r < d \text{ ou } r = 0$$

Alors,

$$q^n - 1 = (q^d - 1)(q^{n-d} + q^{n-2d} + ... + q^{n-qd}) + (q^r - 1)$$

Comme $n - qd = r < d$, cela constitue la division euclidienne de $q^n - 1$ par $q^d - 1$. Comme $q^d - 1 \mid q^n - 1$, on en déduit $q^r - 1 = 0$. D'où $r = 0$ et $d \mid n$.
On a alors

$$|\omega(x) = \frac{|k^\times|}{|k_x^\times|} = \frac{q^n - 1}{q^d - 1} \text{ avec } d \mid n$$

3. On a, dans $\mathbb{Z}$, par une propriété classique des polynômes cyclotomiques :

$$q^n - 1 = \prod_{m|n} \Phi_m(q)$$

Et de même,

$$q^d - 1 = \prod_{m|d} \Phi_m(q)$$

Donc,

$$\frac{q^n - 1}{q^d - 1} = \prod_{m|n, m\nmid d} \Phi_m(q)$$

Pour $d \neq n$, on voit donc en particulier que $\Phi_n(q) \mid \frac{q^n-1}{q^d-1}$.

4. Écrivons désormais l'équation aux classes :

$$|k^\times| = |Z^\times| + \sum_{x \notin Z} |\omega(x)|$$

De plus, dire que $x \notin Z$ signifie que l'on a $d \neq n$, de sorte que

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}$$

la somme portant sur un certain nombre de diviseurs stricts de n. Comme $\Phi_n(q) \mid q^n - 1$ et $\Phi_n(q) \mid \frac{q^n-1}{q^d-1}$ pour un diviseur strict d de n, on en déduit que $\Phi_n(q) \mid q - 1$. En particulier, $|\Phi_n(q)| \leq q - 1$.

5. On a $\Phi_n(q) = (q - \xi_1)...(q - \xi_l)$, où $\xi_1, ..., \xi_l$ sont les racines primitives n-ièmes de l'unité. En particulier, $|\xi_i| = 1$ et $\xi_i \neq 1$ car $n \neq 1$. Mais alors, on a, pour tout i, $|q - \xi_i| > q - 1$ (faire un dessin). Donc, $|\Phi_n(q) > (q - 1)^l \geq q - 1$. Contradiction. ■

Cône nilpotent

Références : Caldero, Germoni, *Histoires hédonistes de groupes et de géométrie - Tome second*, p 213-215

On s'intéresse au nombre d'endomorphisme nilpotents sur un $\mathbb{F}_q$-espace vectoriel de dimension finie d. On notera $\mathcal{N}(E)$ l'ensemble des endomorphisme nilpotent. Un choix de base le met en bijection avec l'ensemble $\mathcal{N}_d(\mathbb{F}_q)$ des matrices nilpotentes de taille d à coefficients dans $\mathbb{F}_q$.

Théorème

Soit E un $\mathbb{F}_q$-espace vectoriel de dimension d. On a :

$$n_d = |\mathcal{N}(E)| = q^{d(d-1)} \quad .$$

Pour $1 \leqslant r \leqslant d$, on pose $L_{r,d}$ l'ensemble des familles des vecteurs de E, libres à r éléments. On dit qu'un endomorphisme nilpotent N *respecte* une famille $\varepsilon \in L_{r,d}$ si pour tout $1 \leqslant i \leqslant r-1$, on a $\varepsilon_{i+1} = N\varepsilon_i$ et $N\varepsilon_r = 0$.

On pose X l'ensemble suivant :

$$X = \{(N, \varepsilon)/N \in \mathcal{N}(E), \exists r, \varepsilon \in L_{r,d} \text{ et } N \text{ respecte } \varepsilon\} \quad .$$

On va dénombrer X de deux manières.

Lemme

Soit $e \in E\backslash\{0\}$ et $N \in \mathcal{N}(E)$, alors il existe un unique r maximal tel que la famille

$$\varepsilon = (e, Ne, \ldots, N^{r-1}e)$$

soit libre. On a de plus : $N^r e = 0$.

Démonstration. L'existence de r est triviale car N est nilpotente. Soit F le sous-espace vectoriel engendré par $\{N^s e/s \in \mathbb{N}\}$. La famille ε est libre dans F. Montrons qu'elle est génératrice. La famille $(e, Ne, \ldots, N^r e)$ est liée, il existe donc une famille de scalaire $(a_i)_{0 \leqslant i \leqslant r}$ non tous nuls telle que : $\sum_{i=0}^{r} a_i N^i e = 0$. Par liberté de ε, a_r ne peut-être nul. On le supposera donc égal à 1. On a donc : $N^r e = -\sum_{i=0}^{r-1} a_i N^i e$.

Pour $s = r + k$, on montre par récurrence sur k que $N^s e \in \text{Vect}(\varepsilon)$. En effet, on a : $N^s e = -\sum_{i=0}^{r-1} a_i N^{i+k} e$. La famille ε est donc une base de F.
On considère la restriction de N à F, notée $\tilde{N}$. C'est un endomorphisme nilpotent. Dans la base ε, sa matrice est la matrice compagnon suivante :

$$\begin{pmatrix} 0 & 0 & \ldots & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{r-1} \end{pmatrix}$$

Son polynôme caractéristique est donc : $\chi_{\tilde{N}} = X^r + \sum_{i=0}^{r-1} a_i X^i$. Comme $\tilde{N}$ est nilpotent, on a donc $a_i = 0$ pour tout $0 \leqslant i \leqslant r-1$. Donc $N^r e = 0$ □

Remarques : • On rappelle que pour calculer g_r, il faut compter le nombre de bases possibles. On a donc

$$g_r = \prod_{r=0}^{d-1}(q^d - q^r) = \prod_{r=0}^{d-1} q^r \times \prod_{r=1}^{d}(q^r - 1) = q^{d(d-1)/2} \prod_{r=1}^{d}(q^r - 1).$$

Adapté du travail de Baptiste Huguet.