Chapitre I

Algèbre linéaire

I.1. Sur les endomorphismes diagonalisables

I.1.1. Endomorphismes diagonalisables et sous-espaces stables

On sait qu'un endomorphisme u est semi-simple si tout sous-espace vectoriel stable par u admet un supplémentaire stable ([Fr. A.] 5.6. p. 221). Ici on suppose que tout sous-espace admet un supplémentaire stable, alors cela est équivalent à u est diagonalisable.

Lemme. *Soient K un corps commutatif, E un K-espace vectoriel de dimension finie, $u \in \mathrm{End}\, E$. Alors les propriétés suivantes sont équivalentes.*
i) L'endomorphisme u est diagonalisable,
ii) tout sous-espace vectoriel de E admet un supplémentaire stable.

Démonstration
1) *Montrons que i) implique ii) .*
Soient F un sous-espace vectoriel de E , $(f_1, f_2, \ldots, f_r)$ une base de F , enfin $(e_1, e_2, \ldots, e_n)$ une base de E qui diagonalise u . Puisque $(e_1, e_2, \ldots, e_n)$ engendre E , on peut extraire une famille $(e_{i1}, e_{i2}, \ldots, e_{in-r})$ de $(e_1, e_2, \ldots, e_n)$ de façon que $(f_1, f_2, \ldots, f_r, e_{i1}, e_{i2}, \ldots, e_{in-r})$ soit une base de E
(Fr. A. Théorème 1.0.2.3.) . Alors $Ke_{i1} \oplus Ke_{i2} \oplus \ldots \oplus Ke_{in-r}$ est clairement un supplémentaire de F qui est stable sous u .
2) *Montrons que ii) implique i) .*
Soit H_1 un hyperplan de E , on a donc un supplémentaire Ke_1 de dimension 1 , stable par u , ce qui veut dire que $u(e_1) = \lambda_1 e_1$.

On considère l'hypothèse de récurrence HRk suivante : il existe une famille libre $(e_1, e_2, \dots, e_k)$ telle que $u(e_i) = \lambda_i e_i$ pour $1 \le i \le k$.
Ce qui précède montre que HR1 est vérifiée.
Montrons que si $k < \dim E$, alors HRk implique HRk+1.
Comme $\dim(Ke_1 \oplus Ke_2 \oplus \dots \oplus Ke_k) < \dim \mathrm{E}$, il existe un hyperplan H de E avec $Ke_1 \oplus Ke_2 \oplus \dots \oplus Ke_k \subset H$. Par *ii)* il existe Ke_{k+1} un supplémentaire de H, de dimension 1 et stable par u, ce qui veut dire que $u(e_{k+1}) = \lambda_{k+1} e_{k+1}$.
Cela montre bien que $(e_1, e_2, \dots, e_k, e_{k+1})$ est une famille libre et que $u(e_i) = \lambda_i e_i$ pour $1 \le i \le k+1$. Ainsi HRk+1 est satisfait et donc HRn est satisfait, ce qui n'est autre chose que *i)*, i.e. que $(e_1, e_2, \dots, e_n)$ diagonalise u.

I.1.2. Matrices circulantes diagonalisables

Proposition. *Soient K un corps commutatif, $a_0, a_1, \dots, a_{n-1} \in K$, la matrice $M := M(a_0, a_1, \dots, a_{n-1}) \in M_n(K)$ définie par*

$$M := \begin{bmatrix} a_0 & a_{n-1} & . & . & a_1 \\ a_1 & a_0 & . & . & a_2 \\ . & . & . & . & . \\ . & . & . & . & a_{n-1} \\ a_{n-1} & a_{n-2} & . & . & a_0 \end{bmatrix}$$

est appelée matrice circulante. Soit

$$J := \begin{bmatrix} 0 & 0 & . & . & 1 \\ 1 & 0 & . & . & 0 \\ . & 1 & . & . & . \\ . & . & . & . & 0 \\ 0 & 0 & . & 1 & 0 \end{bmatrix}$$

la matrice compagnon de $X^n - 1$, qui est aussi la matrice associée à la permutation circulaire $(1, 2, \dots, n)$; ce qui veut dire que si $(\varepsilon_k)_{1 \le k \le n}$ est la base canonique de K^n, on a $J\varepsilon_k = \varepsilon_{k+1}$ pour $1 \le k < n$ et $J\varepsilon_n = \varepsilon_1$. Si donc $\chi_J(X)$ est le polynôme caractéristique de J et $m_J(X)$ le polynôme minimal de J, on a $\chi_J(X) = m_J(X) = X^n - 1$.
1. *Si donc $P(X) := a_0 + a_1 X + \dots + a_{n-1} X^{n-1}$, on a $M(a_0, a_1, \dots, a_{n-1}) = P(J)$. Il suit de cela que $P \mapsto P(J)$ est une bijection linéaire de l'espace vectoriel des polynômes de $K[X]$, de degré strictement inférieur à n sur le sous-espace vectoriel des matrices circulantes de $M_n(K)$. En particulier l'espace vectoriel des matrices circulantes de $M_n(K)$ est de dimension n.*

2. Le déterminant d'une matrice circulante. *Soit* K^{alg} *une clôture algébrique de* K *, alors le polynôme caractéristique de* J *admet une factorisation sous la forme*

$$\chi_J(X)=X^n-1=(X-x_1)(X-x_2)\dots(X-x_n)$$

avec $x_i\in K^{alg}$ *. Si donc* $M=P(J)$ *, on a* $\det M=P(x_1)P(x_2)\dots P(x_n)$ *.*

3. Les matrices circulantes diagonalisables.

On suppose que $n1_K\neq 0$ *, cela veut dire que* $\operatorname{car}K=0$ *ou que* $\operatorname{car}K=p$ *avec* p *premier et* $p\nmid n$ *. Il suit de cela que* $\chi_J(X)=m_J(X)=X^n-1$ *admet une factorisation de la forme*

$$(X-x_1)(X-x_2)\dots(X-x_n) \text{ avec } x_i\in K^{alg} \text{ et } x_i\neq x_j \text{ si } i\neq j .$$

Soit $P(X)\in K[X]$ *avec* $\deg P(X)<n$ *, alors on a les propriétés équivalentes suivantes.*

i) La matrice $M:=P(J)$ *est un élément diagonalisable de* $M_n(K)$ *,*

ii) on a $P(x_i)\in K$ *pour* $1\leq i\leq n$ *.*

4. *On suppose toujours que* $n1_K\neq 0$ *. Alors on a*

$X^n-1=P_1(X)P_2(X)\dots P_r(X)$ *avec* $P_i(X)\in K[X]$ *,* $P_i(X)$ *est irréductible unitaire de* $K[X]$ *pour* $1\leq i\leq r$ *et bien sûr* $P_i(X)\neq P_j(X)$ *si* $i\neq j$ *.*

4.1. *Alors les matrices circulantes de* $M_n(K)$ *qui sont des éléments diagonalisables de* $M_n(K)$ *constituent un sous–espace vectoriel de dimension* r *.*

4.2. *Soit* $M=P(J)$ *avec* $P(X)\in K[X]$ *et* $\deg P<n$ *, une matrice circulante qui est un élément diagonalisable de* $M_n(K)$ *. Il suit de* **3.** *que*

$\operatorname{spectre}M=\{P(x_i)\mid 1\leq i\leq n\}$ *. Soit* $\{y_1,y_2,\dots,y_r\}$ *un sous-ensemble de* $\{x_1,x_2,\dots,x_n\}$ *tel que* $P_j(y_j)=0$ *pour* $1\leq j\leq r$ *.*

Soit $\lambda\in\operatorname{spectre}M$ *,* $I_\lambda:=\{j\mid 1\leq j\leq r \text{ et } P(y_j)=\lambda\}$ *. Alors*

$$\ker(M-\lambda I_n)=\bigoplus_{j\in I_\lambda}\ker P_j(J) .$$

5. *Si* $K=\mathbb{Q}$ *, alors les matrices circulantes de* $M_n(\mathbb{Q})$ *qui sont des éléments diagonalisables de* $M_n(\mathbb{Q})$ *constituent un sous–espace vectoriel de dimension le nombre de diviseur positifs de* n *.*

On a $X^n-1=\prod_{d\mid n}\Phi_d(X)$ *où* $\Phi_d(X)$ *est le* d*-ème polynôme cyclotomique.*

Soit $M=P(J)$ *avec* $P(X)\in\mathbb{Q}[X]$ *et* $\deg P<n$ *, une matrice circulante qui est un élément diagonalisable de* $M_n(\mathbb{Q})$ *. Il suit de* **3.** *que*

$\operatorname{spectre}M=\{P(w)\mid w\in\mathbb{Q}^{alg} \text{ et } w^n=1\}$ *. Soit* $\lambda\in\operatorname{spectre}M$ *,*

$$I_\lambda:=\{d\mid 1\leq d\,,\, d\mid n\,,\, P(w)=\lambda \text{ si } w\in\mathbb{Q}^{alg} \text{ et } o(w)=d\} .$$

Alors $\ker(M-\lambda I_n)=\bigoplus_{d\in I_\lambda}\ker\Phi_d(J)$ *.*

Démonstration

1) La partie 1. est élémentaire.

2) *Montrons* 2. On a donc

$$\chi_J(X)=m_J(X)=X^n-1=(X-x_1)(X-x_2)\dots(X-x_n)$$

avec $x_i\in K^{alg}$. Il suit que J est semblable modulo $G\ell_n(K^{alg})$ à une matrice triangulaire supérieure de diagonale $(x_1, x_2, \dots, x_n)$. Ainsi $P(J)$ est semblable à une matrice triangulaire supérieure de diagonale $(P(x_1), P(x_2), \dots, P(x_n))$, il suit que $\det M=P(x_1)P(x_2)\dots P(x_n)$.

3) *Montrons* 3. Comme J est la matrice compagnon de X^n-1 , on a donc

$$\chi_J(X)=m_J(X)=X^n-1=(X-x_1)(X-x_2)\dots(X-x_n)$$

avec $x_i\in K^{alg}$ et $x_i\neq x_j$ pour $i\neq j$ puisque $n\,1_K\neq 0$. Il suit que J est semblable modulo $G\ell_n(K^{alg})$ à la matrice diagonale, de diagonale $(x_1, x_2, \dots, x_n)$. Ainsi $M:=P(J)$ est semblable à la matrice diagonale, de diagonale $(P(x_1), P(x_2), \dots, P(x_n))$. Soit $\Lambda:=\{P(x_i)\mid 1\le i\le n\}=\text{spectre}\,M$. Ainsi le minimal de M , comme élément de $M_n(K^{alg})$ est $\prod_{\lambda\in\Lambda}(X-\lambda)$. On sait aussi que c'est le minimal de M considéré comme élément de $M_n(K)$ ([Fr. A.] ex. 3.5.1). Si donc M est élément diagonalisable de $M_n(K)$, il suit que $\prod_{\lambda\in\Lambda}(X-\lambda)$ admet une factorisation en polynômes unitaires distincts de $K[X]$, ce qui veut dire que $\lambda\in K$ et donc que $P(x_i)\in K$ pour $1\le i\le n$. Réciproquement si $P(x_i)\in K$ pour $1\le i\le n$, il suit que le polynôme minimal de M considéré comme élément de $M_n(K^{alg})$ est $\prod_{\lambda\in\Lambda}(X-\lambda)$, et comme $\lambda\in K$, il suit que M est un élément diagonalisable de $M_n(K)$ ([Fr. A.] 5.2.2) .

4) *Montrons* 4.

4.1) Montrons 4.1. Il suit de 1. et 3. que si

$$\mathcal{P}:=\{P\in K[X]\mid \deg P<n \text{ et } P(x_i)\in K \text{ pour } 1\le i\le n\},$$

alors l'application $P\mapsto P(J)$ est une bijection linéaire de $\mathcal{P}$ sur l'espace vectoriel des matrices circulantes de $M_n(K)$ qui sont des éléments diagonalisables de $M_n(K)$.

Soit $C_i(X):=A_i(X)\dfrac{X^n-1}{P_i}$, avec $A_i=\dfrac{1}{n}(XP_i'-d_iP_i)$ où d_i est le degré de P_i et P_i' est le polynôme dérivé de P_i .

Il suit de (IV.13) que $(C_1, C_2, \dots, C_r)$ est une base de $\mathcal{P}$; cela montre que les matrices circulantes de $M_n(K)$ qui sont des éléments diagonalisables de $M_n(K)$ constituent un sous-espace vectoriel de dimension r .

4.2) Montrons 4.2. On a $K^n = \bigoplus_{j=1}^{r} \ker P_j(J)$ ([Fr. A.] 3.1.2.).

Par ailleurs, on sait (IV.13) que

(1) $$1 = C_1(X) + C_2(X) + \ldots + C_r(X)$$

Soit $x \in \ker P_1(J)$, comme $P_1 \mid C_j$ pour $2 \le j \le r$, on a donc $C_j(J)(x) = 0$ pour $2 \le j \le r$. Il suit de cela et de (1) que $x = C_1(J)(x)$. De façon analogue,

(2) si $x \in \ker P_j(J)$, on a $C_j(J)(x) = x$ et $C_{j'}(J)(x) = 0$ pour $j' \neq j$.

Si donc P est tel que $P(x_i) \in K$, il suit de (IV.13) que

(3) $$P(X) = P(y_1)\, C_1(X) + P(y_2)\, C_2(X) + \ldots + P(y_r)\, C_r(X)$$

Cela montre que

(4) $$P(J) = P(y_1)\, C_1(J) + P(y_2)\, C_2(J) + \ldots + P(y_r)\, C_r(J) .$$

Il suit de cela et des relations (2) que l'espace propre de $P(J)$ relativement à la valeur propre λ est bien $\bigoplus_{j \in I_\lambda} \ker P_j(J)$.

5) *Montrons* 5.

On a $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ où $\Phi_d(X)$ est le d-ème polynôme cyclotomique.

Il suit que $\mathbb{Q}^n = \bigoplus_{d \mid n} \ker \Phi_d(J)$ ([Fr. A.] 3.1.2.) .

Soit $A_d = \frac{1}{n}(X\Phi_d' - \varphi(d)\,\Phi_d)$ où $\varphi(d)$ est l'indicateur d'**Euler**, c'est aussi le degré de Φ_d et Φ_d' est le polynôme dérivé de Φ_d .

Soit $C_d(X) := A_d(X)\frac{X^n - 1}{\Phi_d}$. Il suit de (IV.13) que $(C_d)_{d \mid n}$ est une base de $\mathcal{P}$.

On a aussi

(5) $$1 = \sum_{d \mid n} C_d(X)$$

(6) Alors $C_d(J)$ induit l'identité sur $\ker \Phi_d(J)$ et l'élément nul sur $\ker \Phi_{d'}(J)$ pour $d \neq d'$.

Soit $M = P(J)$ avec $P(X) \in \mathbb{Q}[X]$ et $\deg P < n$, une matrice circulante qui est un élément diagonalisable de $M_n(\mathbb{Q})$. Il suit de (3) que $P(w) \in \mathbb{Q}$ pour tout $w \in \mathbb{Q}^{alg}$ et $w^n = 1$. Soit $w_d \in \mathbb{Q}^{alg}$ avec $o(w_d) = d$. Soit $\lambda \in \text{spectre}\, M$ et

$$I_\lambda := \{d \mid 1 \le d\,,\ d \mid n\,,\ P(w_d) = \lambda\} .$$

Il suit alors de (6) que l'espace propre de $P(J)$ relativement à la valeur propre λ est $\bigoplus_{d \in I_\lambda} \ker \Phi_d(J)$.

Remarque. Il existe dans $\mathbb{C}^n$ une base de vecteurs propres pour J . A partir de cette dernière, on peut construire une base de $\ker \Phi_d(J)$ dans $\mathbb{Q}^n$ (voir Appendice de IV.13).

I.2. Quelques comptages

I.2.1. Comptage des endomorphismes (resp. automorphismes) diagonalisables

Proposition. *Soient* $\mathbb{F}_q$ *le corps à* q *éléments,* $D_n(\mathbb{F}_q)$ (resp. $E_n(\mathbb{F}_q)$) *le sous-ensemble de* $M_n(\mathbb{F}_q)$ (resp. $G\ell_n(\mathbb{F}_q)$) *des éléments diagonalisables.*

Soit $\sigma:\mathbb{N}\to\mathbb{N}$ *l'application définie par* $\sigma(0)=1$ *et pour* $m\geq 1$ *par*

$$\sigma(m)=o(G\ell_m(\mathbb{F}_q))=(q^m-q)(q^m-q^2)\dots(q^m-q^{m-1})\ .$$

Soit $F:=\{\beta=(\beta_1,\beta_2,\dots,\beta_q)\in\mathbb{N}^q \mid \beta_1+\beta_2+\dots+\beta_q=n\}$ *, alors*

(1) $$\operatorname{card} D_n(\mathbb{F}_q)=\sum_{\beta\in F}\frac{\sigma(n)}{\sigma(\beta_1)\,\sigma(\beta_2)\dots\sigma(\beta_q)}\ .$$

Soit $G:=\{\gamma=(\gamma_1,\gamma_2,\dots,\gamma_{q-1})\in\mathbb{N}^{q-1} \mid \gamma_1+\gamma_2+\dots+\gamma_{q-1}=n\}$ *, alors*

(2) $$\operatorname{card} E_n(\mathbb{F}_q)=\sum_{\gamma\in G}\frac{\sigma(n)}{\sigma(\gamma_1)\,\sigma(\gamma_2)\dots\sigma(\gamma_{q-1})}\ .$$

(1') *Soit* $d_n(\mathbb{F}_q):=\operatorname{card} D_n(\mathbb{F}_q)$ *, alors la formule* (1) *se traduit en terme de série génératrice par*

$$\sum_{k\geq 0}\frac{d_k}{\sigma(k)}X^k=\Big(\sum_{t\geq 0}\frac{1}{\sigma(t)}X^t\Big)^q\ .$$

(2') *Soit* $e_n(\mathbb{F}_q):=\operatorname{card} E_n(\mathbb{F}_q)$ *, alors la formule* (2) *se traduit en terme de série génératrice par*

$$\sum_{k\geq 0}\frac{e_k}{\sigma(k)}X^k=\Big(\sum_{t\geq 0}\frac{1}{\sigma(t)}X^t\Big)^{q-1}\ .$$

Démonstration

La méthode Le groupe $G\ell_n(\mathbb{F}_q)$ opère par conjugaison sur $D_n(\mathbb{F}_q)$, les matrices qui sont un tableau diagonal de matrices de la forme

$$(a_1I_{\alpha_1},a_2I_{\alpha_2},\dots,a_rI_{\alpha_r}) \text{ avec } a_i\in\mathbb{F}_q^*,\ \alpha_i>0 \text{ et } \alpha_1+\alpha_2+\dots+\alpha_r=n\ ,$$

constituent un système de représentants des orbites de $D_n(\mathbb{F}_q)$ sous cette action. Sachant que le stabilisateur (ou sous-groupe d'isotropie) du tableau diagonal $(a_1I_{\alpha_1},a_2I_{\alpha_2},\dots,a_rI_{\alpha_r})$ est l'ensemble des tableaux diagonaux $(S_1,S_2,\dots,S_r)$, avec $S_k\in G\ell_{\alpha_k}(\mathbb{F}_q)$, on en déduit le cardinal de chaque orbite. Et alors la sommation sur les orbites donne le cardinal de $D_n(\mathbb{F}_q)$.

1) *Description des orbites de* $D_n(\mathbb{F}_q)$

1.1) Soient $\mathbb{F}_q=\{x_1,x_2,\dots,x_q\}$,

$F:=\{\beta=(\beta_1,\beta_2,\dots,\beta_q)\in\mathbb{N}^q \mid \beta_1+\beta_2+\dots+\beta_q=n\}$, $\mathcal{P}$ l'ensemble des polynômes unitaires de degré n de $\mathbb{F}_q[X]$ qui se factorisent en polynômes unitaires de degré 1 de $\mathbb{F}_q[X]$. Soit $\theta:\mathcal{P}\to F$ l'application définie par

$\theta(P)=\beta=(\beta_1,\beta_2,\dots,\beta_q)$ où β_i est la multiplicité de x_i dans P ; on a donc $P(X)=\prod_{i=1}^{q}(X-x_i)^{\beta_i}$. Enfin, soit $f:D_n(\mathbb{F}_q)\to F$, défini par $f(A):=\theta(\chi_A(X))$.

1.2) Le représentant Δ_β.

Soient $\beta=(\beta_1,\beta_2,\dots,\beta_q)\in F$ et $i_1<i_2<\dots<i_r$ avec $\beta_{i_1}\geq 1,\beta_{i_2}\geq 1,\dots,\beta_{i_r}\geq 1$ et $\beta_j=0$ si $j\notin\{i_1,i_2,\dots,i_r\}$. Soit Δ_β le tableau diagonal

$$(x_{i_1}I_{\beta_{i_1}},x_{i_2}I_{\beta_{i_2}},\dots,x_{i_r}I_{\beta_{i_r}}),$$

alors $\Delta_\beta\in D_n(\mathbb{F}_q)$ et $f(\Delta_\beta)=\beta$ et on a

$$\chi_{\Delta_\beta}(X)=\prod_{i=1}^{q}(X-x_i)^{\beta_i}.$$

1.3) *Les orbites de $D_n(\mathbb{F}_q)$ sous l'action de $G\ell_n(\mathbb{F}_q)$ sont les orbites des Δ_β pour $\beta\in F$.*

Le groupe $G\ell_n(\mathbb{F}_q)$ opère par conjugaison sur $D_n(\mathbb{F}_q)$, soit $A\in D_n(\mathbb{F}_q)$, alors il suit de 1.1) qu'il existe $\beta\in F$ tel que $f(A)=\beta$. Comme $f(\Delta_\beta)=\beta$, il suit de la définition de f en 1.1) que $\chi_A(X)=\chi_{\Delta_\beta}(X)$; alors le lemme ci-après permet de conclure que Δ_β et A sont dans la même orbite.

Par ailleurs si Δ_β et $\Delta_{\beta'}$ sont dans la même orbite, on a $\chi_{\Delta_\beta}(X)=\chi_{\Delta_{\beta'}}(X)$ et donc $f(\Delta_\beta)=f(\Delta_{\beta'})$ et par 1.2) on a $\beta=\beta'$. Ainsi l'application $\beta\mapsto G\ell_n(\mathbb{F}_q)*\Delta_\beta$ est une bijection de F sur les orbites $D_n(\mathbb{F}_q)$.

1.4) *Le stabilisateur (ou sous-groupe d'isotropie) de Δ_β.*

Selon 1.2) l'élément Δ_β est le tableau diagonal

$$(x_{i_1}I_{\beta_{i_1}},x_{i_2}I_{\beta_{i_2}},\dots,x_{i_r}I_{\beta_{i_r}})$$

avec $i_1<i_2<\dots<i_r$. Sachant que les éléments $i_1,i_2,..,i_r$ sont distincts, il est facile de montrer que les éléments $S\in G\ell_n(\mathbb{F}_q)$ qui commutent avec Δ_β sont les tableaux diagonaux $(S_1,S_2,\dots,S_r)$ avec $S_k\in G\ell_{\beta_{i_k}}(\mathbb{F}_q)$. Ainsi en utilisant la définition de l'application σ, il suit que l'ordre du stabilisateur de Δ_β est $\sigma(\beta_1)\,\sigma(\beta_2)\dots\sigma(\beta_q)$.

1.5) *Le cardinal de $D_n(\mathbb{F}_q)$*

Il suit donc de 1.4) que $\operatorname{card} G\ell_n(\mathbb{F}_q)*\Delta_\beta=\dfrac{\sigma(n)}{\sigma(\beta_1)\,\sigma(\beta_2)\dots\sigma(\beta_q)}$, ainsi

$$\operatorname{card} D_n(\mathbb{F}_q)=\sum_{\beta\in F}\frac{\sigma(n)}{\sigma(\beta_1)\,\sigma(\beta_2)\dots\sigma(\beta_q)}.$$

C'est bien la formule (1).

2) *Description des orbites de $E_n(\mathbb{F}_q)$*

La démonstration est identique à 1). Toutefois il faut remplacer F par

$$G:=\{\gamma=(\gamma_1,\gamma_2,\dots,\gamma_{q-1})\in\mathbb{N}^{q-1}\mid \gamma_1+\gamma_2+\dots+\gamma_{q-1}=n\},$$

il faut remplacer $\mathcal{P}$ par $\mathcal{Q}$, l'ensemble des polynômes unitaires de degré n de $\mathbb{F}_q[X]$, qui ne s'annulent pas en 0 et qui se factorisent en polynômes unitaires de degré 1 de $\mathbb{F}_q[X]$. On suppose aussi que

$$\mathbb{F}_q - \{0\} = (x_1, x_2, \dots, x_{q-1}) .$$

Si $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_{q-1}) \in G$ et $i_1 < i_2 < \dots < i_r$ avec $\gamma_{i_1} \geq 1$, $\gamma_{i_2} \geq 1, \dots, \gamma_{i_r} \geq 1$ et $\gamma_j = 0$ si $j \notin \{i_1, i_2, \dots, i_r\}$. Alors Δ_γ est le tableau diagonal

$$(x_{i_1} I_{\gamma_{i_1}}, x_{i_2} I_{\gamma_{i_2}}, \dots, x_{i_r} I_{\gamma_{i_r}}) .$$

Il suit que les orbites de $E_n(\mathbb{F}_q)$ sous l'action de conjugaison par $G\ell_n(\mathbb{F}_q)$ sont les orbites des Δ_γ et que ces dernières sont en bijection avec G. En plus, l'ordre du stabilisateur de Δ_γ est

$$\sigma(\gamma_1)\, \sigma(\gamma_2) \dots \sigma(\gamma_{q-1}) ,$$

il suit de cela que

$$\operatorname{card} E_n(\mathbb{F}_q) = \sum_{\gamma \in G} \frac{\sigma(n)}{\sigma(\gamma_1)\, \sigma(\gamma_2) \dots \sigma(\gamma_{q-1})} \ ;$$

ce qui est la formule (2).

Lemme

1. *Soient $E \neq \{0\}$ un k-espace vecroriel de dimension finie, $u \in \operatorname{End} E$ un endomorphisme diagonalisable. Alors $\chi_u(X) = (X - a_1)^{\alpha_1} (X - a_2)^{\alpha_2} \dots (X - a_r)^{\alpha_r}$ avec $a_i \neq a_j$ si $i \neq j$ et $\alpha_i \geq 1$ et de plus $\dim \ker(u - a_i \mathbb{1}) = \alpha_i$ pour $1 \leq i \leq r$. Ainsi il existe une base $\mathcal{B}$ de E de façon que $\operatorname{Mat}(u; \mathcal{B})$ soit le tableau diagonal de matrices $(a_1 I_{\alpha_1}, a_2 I_{\alpha_2}, \dots, a_r I_{\alpha_r})$.*

2. *Soient $A, B \in M_n(K)$, des matrices diagonalisables.*

Alors les propriétés suivantes sont équivalentes.

i) A est semblable à B, ii) $\chi_A(X) = \chi_B(X)$.

Démonstration

1) Le 1. est le théorème 5.2.2. (Fr. A. p. 213).

2) Pour le 2., *i)* implique *ii)* est immédiat.

Si $\chi_A(X) = \chi_B(X) = (X - a_1)^{\alpha_1} (X - a_2)^{\alpha_2} \dots (X - a_r)^{\alpha_r}$ avec $a_i \neq a_j$ si $i \neq j$ et $\alpha_i \geq 1$. Il suit alors de 1. que A (resp. B) est semblable à la matrice qui est le tableau diagonal $(a_1 I_{\alpha_1}, a_2 I_{\alpha_2}, \dots, a_r I_{\alpha_r})$; donc A et B sont semblables.

I.2.2. Comptage des matrices de rang r de $M_{n,m}(\mathbb{F}_q)$

Proposition. *Soit $\mathbb{F}_q$ le corps à q éléments, alors le nombre de matrices de $M_{n,m}(\mathbb{F}_q)$ qui sont de rang r est*

$$\frac{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-r+1} - 1)}{(q^r - 1)(q^{r-1} - 1) \dots (q - 1)} (q^m - 1)(q^{m-1} - 1) \dots (q - 1)\, q^{\frac{r(r-1)}{2}} .$$