réf : [ROM] §5.6 pp. 148-151 (dénombrement des automorphismes)
[H2G2] Tome 1 §VIII pp. 264-265 (très elliptique)

leçons :
101
155
190
(123)
(154)
150

Dénombrement des endomorphismes diagonalisables d'un espace vectoriel de corps de base fini

Soient $\mathbb{K}$ un corps fini de cardinal $q \in \mathbb{N}$
E un $\mathbb{K}$ espace vectoriel de dimension $n \in \mathbb{N}^*$

Le nombre d'endomorphismes diagonalisables sur E est :
$$\sum_{\substack{(m_1,\dots,m_q)\in\mathbb{N}^q \\ m_1+\dots+m_q=n}} \frac{|GL_n \mathbb{F}_q|}{\prod_{i=1}^{q} |GL_{m_i} \mathbb{F}_q|}$$
avec par convention d'écriture : $|GL_0 \mathbb{F}_q| = 1$

Notons $\mathcal{D}(E)$ l'ensemble des endomorphismes diagonalisables de E.

Lemme $\mathcal{D}(E) = \{ u \in \mathcal{L}(E) \mid u^q = u \}$

long

Numérotons les q éléments de $\mathbb{K}$:
$\mathbb{K} = \{\lambda_1, \dots, \lambda_q\}$.
Un endomorphisme $u \in \mathcal{L}(E)$ est diagonalisable si et seulement s'il est annulé par un polynôme de $\mathbb{K}[X]$ scindé à racines simples. Donc :

- si $u \in \mathcal{D}(E)$: $\exists P \in \mathbb{K}[X], \begin{cases} P(u) = 0 \\ P \mid \prod_{i=1}^{q} X - \lambda_i \end{cases}$

or $\prod_{i=1}^{q} X - \lambda_i = X^q - X$

donc $u^q = u$,

et réciproquement :

- si $u^q = u$: le polynôme $X^q - X \in \mathbb{K}[X]$ annule u et est scindé à racines simples, donc u est diagonalisable.

Étape 1

$$\boxed{\forall u \in \mathcal{D}(E) : \quad E = \bigoplus_{i=1}^{q} \ker(u - \lambda_i \, id_E)}$$

ne pas écrire

Si $u \in \mathcal{D}(E)$, $X^q - X = \prod_{i=1}^{q} X - \lambda_i$ annule u, et les $(X - \lambda_i)_{1 \leq i \leq q}$ sont premiers entre eux, donc d'après le lemme des noyaux :

$$E = \bigoplus_{i=1}^{q} \ker(u - \lambda_i \, id_E)$$

Étape 2

Posons $\mathcal{P}_E = \{ (E_1, \dots, E_q) \text{ sev de } E \mid E = \bigoplus_{i=1}^{q} E_i \}$.

La correspondance

$$\Phi : \begin{cases} \mathcal{D}(E) \longrightarrow \mathcal{P}_E \\ u \longmapsto (\ker(u - \lambda_i \, id_E))_{1 \leq i \leq q} \end{cases}$$

est une bijection.

Grâce à l'étape 1, notons que Φ est bien définie.

injectivité

- Soient $u, v \in \mathcal{D}(E)$ tels que $\Phi(u) = \Phi(v)$.

Alors en notant $E_i = \ker(u - \lambda_i \, id_E) = \ker(v - \lambda_i \, id_E)$:

on a : $u_{|E_i} = \lambda_i \, id_{E_i} = v_{|E_i}$ $\forall i \in [\![1 ; q]\!]$,

donc, comme $E = \bigoplus_{i=1}^{q} E_i$, $u = v$

et $\underline{\Phi \text{ est injectif}}$.

surjectivité · Soit $\mathcal{E} = (E_1, \dots, E_q) \in \mathcal{O}\ell$.

Alors l'endomorphisme $u \in \mathcal{L}(E)$ défini par

$$u(x) = \lambda_i x \quad \forall x \in E_i \quad \forall i \in [\![1;q]\!]$$

est diagonalisable avec $\ker(u - \lambda_i id_E) = E_i$.

Donc $\Phi(u) = \mathcal{E}$ et Φ est surjectif.

Étape 3 Dénombrons $\mathcal{O}\ell$ grâce à l'action naturelle de $GL(E)$ définie par :

$$u \cdot (E_1, \dots, E_q) = (u(E_1), \dots, u(E_q))$$

où on a bien $E = \bigoplus_{i=1}^{q} u(E_i)$ car $u \in GL(E)$.

· Soit $\mathcal{E} = (E_1, \dots, E_k) \in \mathcal{O}\ell$ et décrivons l'orbite $Orb\,\mathcal{E}$ de $\mathcal{E}$ sous cette action :

on a $\underline{Orb\,\mathcal{E} = \{(F_1, \dots, F_q) \in \mathcal{O}\ell \mid \dim F_i = \dim E_i \ \forall i\}}$.

En effet, si $u \in GL(E)$: $\dim u(E_i) = \dim E_i \ \forall i$;

et si $(F_1, \dots, F_q)$ est dans le membre de droite : soient $\mathcal{B} = \bigcup_{i=1}^{q} \mathcal{B}_i$ et $\mathcal{B}' = \bigcup_{i=1}^{q} \mathcal{B}'_i$ des bases adaptées à $\mathcal{E}$ et $(F_1, \dots, F_q)$ respectivement, l'automorphisme $u \in GL(E)$ défini par

$$u(\mathcal{B}_i) = \mathcal{B}'_i \quad \forall i$$

vérifie $u \cdot \mathcal{E} = (F_1, \dots, F_q)$.

· Décrivons maintenant le stabilisateur d'un élément $\mathcal{E} = (E_1, \dots, E_q) \in \mathcal{O}\ell$ noté $Stab\,\mathcal{E}$.

On a $\text{Stab}\,\mathcal{E} = \{u \in GL(E) \mid u(E_i) = E_i \ \forall i\}$
$= \{u \in GL(E) \mid u_{|E_i} \in GL(E_i) \ \forall i\}$
(où (par convention) $GL\{0\}$ est trivial)
donc $\text{Stab}\,\mathcal{E}$ est isomorphe à $\prod_{i=1}^{q} GL(E_i)$.

Donc l'équation aux classes donne :

$$|\mathcal{O}_\mathcal{E}| = \sum_{\omega \in \mathcal{O}_\mathcal{E}/GL(E)} |\omega| = \sum_{\mathcal{E} \in \mathcal{R}} \frac{|GL(E)|}{|\text{Stab}\,\mathcal{E}|}$$

où $\mathcal{R}$ est un ensemble de représentants des orbites,
mais alors $\mathcal{R} \simeq \mathcal{O}_\mathcal{E}/GL(E) \simeq \{(m_1,\dots,m_q) \in \mathbb{N}^q \mid n = \sum_1^q n_i\}$
où $\mathcal{E} \longmapsto \text{Orb}\,\mathcal{E} \longmapsto (\dim E_i)_{1 \le i \le q}$

donc :

$$|\mathcal{O}_\mathcal{E}| = \sum_{\substack{(m_1,\dots,m_q) \in \mathbb{N}^q \\ m_1 + \dots + m_q = n}} \frac{|GL_n \mathbb{F}_q|}{\prod_{i=1}^{q} |GL_{m_i} \mathbb{F}_q|}$$

et comme $|\mathcal{D}(E)| = |\mathcal{O}_\mathcal{E}|$ on a le résultat.

Autre version : Dénombrement des automorphismes diagonalisables

Mêmes arguments, en montrant :

① $\mathcal{D}(E) \cap GL(E) = \{u \in \mathcal{L}(E) \mid u^{q-1} = id_E\}$

② $\mathcal{D}(E) \cap GL(E) \simeq \{(E_1,\dots,E_{q-1}) \mid E = \bigoplus_{i=1}^{q-1} E_i\} = \widetilde{\mathcal{O}_\mathcal{E}}$
(en remarquant $E = \bigoplus_{\lambda \in \mathbb{F}_q^\times} \ker(u - \lambda\, id_E)$ $\forall u \in \mathcal{D}(E) \cap GL(E)$)

③ $\widetilde{\mathcal{O}_\mathcal{E}}/GL(E) \simeq \{(m_1,\dots,m_{q-1}) \in \mathbb{N}^{q-1} \mid n = \sum_1^{q-1} m_i\}$

$$\Rightarrow \quad |\mathcal{D}(E) \cap GL(E)| = \sum_{\substack{(m_1,\dots,m_{q-1}) \in \mathbb{N}^{q-1} \\ m_1 + \dots + m_{q-1} = n}} \frac{|GL_n \mathbb{F}_q|}{\prod_{i=1}^{q-1} |GL_{m_i} \mathbb{F}_q|}$$

+ on peut montrer que $|\mathcal{D}(E)|$ est un polynôme en q