~15 min oh
15 min rapide

NOMBRE D'AUTOMORPHISMES DIAGONALISABLES SUR UN CORPS FINI.

Gourdon Algèbre
adaptation FGN Alg 1. 1.10

Prérequis : × diagonalisat° et polynôme scindé à racines simples, lemme des noyaux voir H2G2 p264.
× action de groupe, transitive, relat° orbite stabilisateur.
× GL envoie toute base sur une base. Si u envoie une base sur une base alors $u \in GL$.

Soit $n \in \mathbb{N}^*$, soit $\mathbb{F}_q$ un corps fini. Soit E un $\mathbb{F}_q$-ev de dimension n.
On note $D(n,q) = \{u \in GL(E),\ u$ diagonalisable $\}$.

Théorème : On a $\displaystyle |D(n,q)| = \sum_{\substack{(n_1,\dots,n_{q-1}) \in \mathbb{N}^{q-1} \\ \sum n_k = n}} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{n_1}(\mathbb{F}_q)| \cdots |GL_{n_{q-1}}(\mathbb{F}_q)|}$

Étape 1 : $D(n,q) = \{u \in GL(E),\ u^{q-1} = id\}$. ex 2 p 179 Gourdon

• Soit $u \in D(n,q)$, alors u est diagonalisable donc son polynôme minimal Π_u est scindé à racines simples. Or $Sp(u) \subset \mathbb{F}_q^*$ ← $u \in GL(E)$ donc $0 \notin Sp(u)$

donc $\Pi_u = \prod_{\lambda \in Sp(u)} (X-\lambda) \ \Big| \ \prod_{\xi \in \mathbb{F}_q^*} (X - \xi) = X^{q-1} - 1$. donc $X^{q-1}-1$ annule u i.e. $u^{q-1} = id$.

Si on note $\xi_1, \dots, \xi_{q-1}$ les élts de $\mathbb{F}_q^*$, alors $\forall i$ $\xi_i^q = \xi_i$ et donc $\xi_i^{q-1} = 1$, on a donc $q-1$ racines de $X^{q-1}-1$ qui est de deg $q-1$ or $\mathbb{F}_q$ est un corps donc $X^{q-1}-1 = \prod_{i=1}^{q-1} (X - \xi_i)$

• Réciproquement, soit $u \in GL(E)$ tel que $u^{q-1} = id$ alors u est annulé par $X^{q-1}-1$ qui est scindé à racines simples donc u est diagonalisable i.e. $u \in D(n,q)$.

Dans la suite, on note $\mathbb{F}_q^* = \{\xi_1, \dots, \xi_{q-1}\}$

Étape 2 : Pour $u \in D(n,q)$, $E = \bigoplus_{k=1}^{q-1} \ker(u - \xi_k id)$.

On a $X^{q-1} - 1 = \prod_{k=1}^{q-1} (X - \xi_k)$ et les $(X - \xi_k)$ sont premiers entre eux donc, d'après le lemme des noyaux, $E = \bigoplus_{k=1}^{q-1} \ker(u - \xi_k id)$ puisque $X^{q-1}-1$ annule u d'après l'étape 1.

On note $\mathcal{F}$ l'ensemble des suites $(E_k)_{1 \le k \le q-1}$ de sev de E tq $E = \bigoplus_{k=1}^{q-1} E_k$

Étape 3 : $\varphi : \begin{array}{ccc} D(n,q) & \longrightarrow & \mathcal{F} \\ u & \longmapsto & (\ker(u - \xi_k id))_{1 \le k \le q-1} \end{array}$ est bijective.

• D'après l'étape 2, φ est bien définie
• injectivité : soient $u, v \in D(n,q)$ tq $\varphi(u) = \varphi(v)$ alors $\forall k \in [\![1, q-1]\!]$,

$\ker(u - \xi_k id) = \ker(v - \xi_k id)$ donc $\forall k \in [\![1, q-1]\!]$, $\forall x \in \ker(u - \xi_k id)$, $u(x) = \xi_k x = v(x)$
or $E = \bigoplus_{k=1}^{q-1} \ker(u - \xi_k id)$ donc $u = v$.

• surjectivité : Soit $(E_k)_{1 \le k \le q-1} \in \mathcal{F}$. On définit u par $\forall k \in [\![1, q-1]\!]$ $u_{|E_k} = \xi_k id_{E_k}$
alors u est complètement déterminée car $E = \bigoplus_{k=1}^{q-1} E_k$, $u \in GL_n(\mathbb{F}_q)$ (car $\xi_k \in \mathbb{F}_q^*$) et
$u^{q-1} = id$ car c'est vrai sur tous les E_k donc $u \in D(n,q)$. par étape 1.

Pour $N = (n_1, \dots, n_{q-1}) \in \mathbb{N}^{q-1}$ tq $\sum_{k=1}^{q-1} n_k = n$, on note $\mathcal{F}_N = \{(E_k)_{1 \le k \le q-1} \in \mathcal{F},\ \dim E_k = n_k\ \forall k \in [\![1, q-1]\!]\}$

Etape 4 : On partitionne.

. Les $(F_N)_{\substack{N\in\mathbb{N}^{q-1}\\ \sum n_k=n}}$ forment une partition de F.

Etape 5 : Pour $N=(n_1,\dots,n_{q-1})\in\mathbb{N}^{q-1}$ tq $\sum n_k=n$, $\begin{array}{rcl} GL_n(\mathbb{F}_q)\times F_N & \longrightarrow & F_N \\ (u,(E_k)) & \longmapsto & (u(E_k)) \end{array}$ définit une action de groupe transitive.

- soit $u\in GL_n(\mathbb{F}_q)$, soit $(E_k)\in F_N$, alors $\underset{u\in GL(E)}{E=u(E)}=\underset{E=\oplus E_k \text{ + u est linéaire}}{\bigoplus_{k=1}^{q-1}u(E_k)}$

  et comme $u\in GL(E)$, $\dim u(E_k)=\dim E_k$ pour $1\leq k\leq q-1$ donc $(u(E_k))_{1\leq k\leq q-1}\in F_N$.

L'application est donc bien définie.

- Cela définit bien une action de groupe.

- Transitivité : Soient (E_k), (E'_k) deux éléments de F_N.
  Pour $k\in[\![1,q-1]\!]$, soient B_k (resp B'_k) une base de E_k (resp E'_k).

  Alors B (resp B') qui est la concaténation des B_k (resp B'_k) est une base de E adaptée à la décomposition en somme directe.

  Comme $\dim E_k=\dim E'_k$, on peut définir $u\in GL(E)$ tq $u(E_k)=E'_k$:

On a $B_k=(f_1,\dots,f_{n_k})$, $B'_k=(f'_1,\dots,f'_{n_k})$, on définit $u : f_i\mapsto f'_i$ alors $u\in GL(E)$ car u envoie une base sur une autre et $u(E_k)=E'_k$

Etape 6 : $|\mathrm{Stab}(E_i)|=\prod_{k=1}^{q-1}|GL_{n_k}(\mathbb{F}_q)|$

$\begin{array}{rcl}\mathrm{Stab}(E_i) & \longrightarrow & \bigotimes_{k=1}^{q-1} GL_{n_k}(\mathbb{F}_q) \\ u & \longmapsto & (u_{|E_i}) \end{array}$ est bijective

On a $\mathrm{Stab}((E_i))=\{u\in GL_n(\mathbb{F}_q),\ \forall i\in[\![1,q-1]\!]\ u(E_i)=E_i\}$.

- soit $u\in\mathrm{Stab}((E_i))$ alors $u(E_i)=E_i$ pour tout $i\in[\![1,q-1]\!]$ donc $u_{|E_i}\in GL(E_i)$.
- soit $u\in GL(E)$ tq $\forall i$ $u_{|E_i}\in GL(E_i)$ alors $u(E_i)=E_i$ pr $\forall i$.

donc si B est une base adaptée à la décomposit° en somme directe, $\mathcal{M}_B(u)=\begin{pmatrix} M_1 & & 0\\ & \ddots & \\ 0 & & M_{q-1}\end{pmatrix}$

où $M_i=\mathcal{M}_{B_i}(u_{|E_i})\in GL_{n_i}(\mathbb{F}_q)$.

Etape 7 : Relation orbite-stabilisateur et conclusion.

On a ; pour $(E_k)\in F_N$, $|\mathrm{Orb}((E_k))|=\dfrac{|GL_n(\mathbb{F}_q)|}{|\mathrm{Stab}((E_k))|}$

Or l'action est transitive donc $\mathrm{Orb}((E_k))=F_N$. Et, comme F se décompose en une partition,

$$|D(n,q)|=|F|=\sum_{\substack{(n_1,\dots,n_{q-1})\in\mathbb{N}^{q-1}\\ \sum n_k=n}}|F_N|=\sum_{\substack{(n_1,\dots,n_{q-1})\in\mathbb{N}^{q-1}\\ \sum n_k=n}}\frac{\cancel{|GL(E)|}\ |GL_n(\mathbb{F}_q)|}{|GL_{n_1}(\mathbb{F}_q)|\cdots|GL_{n_{q-1}}(\mathbb{F}_q)|}$$

$$|\{A\in\mathcal{M}_n(\mathbb{F}_q),\ A \text{ diagonalisable}\}|=\sum_{\substack{(n_1,\dots,n_q)\in\mathbb{N}^q\\ \sum n_q=n}}\frac{|GL_n(\mathbb{F}_q)|}{|GL_{n_1}(\mathbb{F}_q)|\cdots|GL_{n_q}(\mathbb{F}_q)|}$$

en décomposant A en son noyau et sa partie inversible $(n_1,\dots,n_{q-1})$

Et $|GL_n(\mathbb{F}_q)|=(q^n-1)\cdots(q^n-q^{n-1})$