$$|D_n(\mathbf{F}_q)| = \sum_{\substack{n_1+\cdots+n_q=n \\ n_i\geq 0}} \frac{g_n}{\prod_{i=1}^q g_{n_i}} \underset{q\to+\infty}{\sim} \frac{q^{n^2}}{n!}$$

Soient n un entier naturel et q une puissance d'un nombre premier. On appellera *partition* un q-uplet de naturels de somme n (la définition classique de la partition est un uplet d'entiers décroissants de somme n ; dans notre définition, on omet la condition sur l'ordre). On note $\mathbf{K} = \mathbf{F}_q$, $\mathcal{N}$ l'ensemble des partitions, et g_n le cardinal de $\mathbf{GL}_n(\mathbf{K})$ que l'on supposera connu. Rappelons enfin que l'ensemble des endomorphismes de $\mathbf{K}^n$ est canoniquement (car l'espace contient une base canonique) isomorphe à l'ensemble des matrices inversibles.
Soit ν une partition, et E_ν l'ensemble

$$E_\nu = \{(E_1, \ldots, E_q)\text{sev de } \mathbf{K}^n \text{ tq. } E_1 \oplus \cdots \oplus E_q = \mathbf{K}^n \text{ et} \dim E_i = n_i \ \forall i\}$$

Lemme : *Les ensembles $D(\mathbf{K}^n)$ et $\bigsqcup_{\nu\in\mathcal{N}} E_\nu$ sont en bijection.*

Démonstration : Ordonnons les éléments de $\mathbf{K}$: $\lambda_1, \ldots, \lambda_q$.

Soit Φ l'application qui à un endomorphisme diagonalisable f associe

$$(\mathrm{Ker}(f - \lambda_1 \mathrm{Id}), \ldots, \mathrm{Ker}(f - \lambda_q \mathrm{Id})) \in \bigsqcup_\nu E_\nu$$

Réciproquement, si $(E_1, \ldots, E_q) \in \bigsqcup_\nu E_\nu$, on construit l'endomorphisme f tel que $f(x) = \lambda_i x$ pour $x \in E_i$. Il est immédiat qu'on a ainsi définit l'inverse de Φ.

Φ réalise donc une bijection entre l'ensemble des endomorphismes diagonalisables et $\bigsqcup_{\nu\in\mathcal{N}} E_\nu$.

□

En particulier $|D_n(\mathbf{K})| = \sum_{\nu\in\mathcal{N}} |E_\nu|$.

Reste à trouver le cardinal de E_ν. C'est là qu'intervient l'action du groupe linéaire.

Proposition : $\mathbf{GL}(\mathbf{K}^n)$ *agit transitivement sur E_ν.*

Démonstration : Posons $g \cdot (E_1, \ldots, E_q) = (g(E_1), \ldots, g(E_q))$.

Axiome 1 : $Id \cdot (E_1, \ldots, E_q) = (E_1, \ldots, E_q)$
Axiome 2 : $g_1 \cdot (g(E_1), \ldots, g(E_q)) = ((g_1 \circ g(E_1), \ldots, g_1 \circ g(E_q)) = (g_1 \circ g) \cdot (E_1, \ldots, E_q)$.

Vérifions à présent que $(g(E_1), \ldots, g(E_q)) \in E_\nu$.
g est un isomorphisme donc g préserve les dimensions. Il suffit donc de montrer que $g(E_i) \cap \sum_{j\neq i} g(E_j) = \{0\}$. Or si x est dans le membre de gauche alors $g^{-1}(x) \in E_i \cap \sum_{j\neq i} E_j = \{0\}$ donc $x = 0$ par injectivité de g^{-1}.

Donc

$$\mathbf{GL}(\mathbf{K}^n) \circlearrowright E_\nu$$

Transitivité : Soient $(E_1, \ldots, E_q), (E'_1, \ldots, E'_q)$ deux éléments de E_ν.
En notant B et B' deux bases de $\mathbf{K}^n$ adaptées à ces sev, l'isomorphisme g envoyant B sur B' envoie le premier q-uplet sur le second.

□

Par transitivité il n'y a qu'une orbite d'où, en notant $E = (E_1, \ldots, E_q)$ un élément quelconque de E_ν :

$$|E_\nu| = \frac{|\mathbf{GL}_n(\mathbf{K})|}{|Stab_E|}$$

Or $g \in Stab_E \Leftrightarrow g(E_i) = E_i \ \forall i \Leftrightarrow g \in Gl(E_i) \ \forall i \Leftrightarrow g$ se représente - dans une base adaptée à E - par une matrice diagonale par blocs inversibles de tailles $n_1, \ldots, n_q$.

Ainsi

$$|E_\nu| = \frac{g_n}{\prod_{i=1}^q g_{n_i}}$$

Autrement dit,

$$|D_n(\mathbf{F}_q)| = \sum_{\substack{n_1+\cdots+n_q=n \\ n_i\geq 0}} \frac{g_n}{\prod_{i=1}^q g_{n_i}}$$

Afin obtenir l'équivalent, on va regrouper dans la somme certains termes qui se ressemblent. Pour ce faire, on considère une partition $(n_1, \ldots, n_q)$ et on note m le nombre de termes non nuls de cette partition : $1 \leq m \leq n$. De cette partition, on extrait les termes non nuls, en conservant leur ordre, c'est-à-dire qu'on associe $(n_{i_1}, \ldots, n_{i_m})$ avec $i_1 < \cdots < i_m$.

Combien d'antécédents possède cette nouvelle partition ? On doit placer $q-m$ zéros, puis boucher les trous en plaçant n_{i_1} à la première place vide, n_{i_2} à la seconde, etc. Il y a donc $\binom{q}{q-m} = \binom{q}{m}$ antécédents.
Chacun de ces antécédents donne le même terme dans la somme. Une nouvelle formule en résulte :

$$|D_n(\mathbf{K})| = \sum_{m=1}^{n} \binom{q}{m} \sum_{\substack{n_1+\cdots+n_m=n \\ n_i>0}} \frac{g_n}{\prod_{i=1}^m g_{n_i}}$$

Cette somme double comprend un nombre fini de termes, et on rappelle que $g_n = (q^n-1)(q^n-q)\ldots(q^n-q^{n-1})$ et $\binom{q}{m} = \frac{q(q-1)\ldots(q-m+1)}{m!}$.
$|D_n(\mathbf{K})|$ est donc une fraction rationnelle en q (en fait, c'est même un polynôme) ; et est ainsi équivalent à son terme dominant.

Le degré du terme $\binom{q}{m}\frac{g_n}{\prod_{i=1}^m g_{n_i}}$ est

$$m + n^2 - \sum_i n_i^2 \leq n + n^2 - \sum_i n_i^2 \leq n + n^2 - \sum_i n_i = n^2$$

La dernière égalité vient du fait que $\sum_i n_i = n$.
La première inégalité est une égalité lorsque $m = n$, la seconde en est une lorsque tous les n_i valent 1, c'est-à-dire lorsque $m = n$.
Le terme correspondant à $m = n$ est

$$\frac{q(q-1)\ldots(q-n+1)}{n!}\frac{g_n}{(q-1)^n} \sim \frac{q^n}{n!}\frac{q^{n^2}}{q^n} = \frac{q^{n^2}}{n!}$$

□

Quelques remarques

Pourquoi la fraction rationnelle $|D_n(\mathbf{K})|$ est-elle un polynôme ? Si on la note $\frac{A(q)}{B(q)}$ avec $A, B \in \mathbf{Z}[X]$, on peut diviser A par B DANS $\mathbf{Z}[X]$ (car B est unitaire) d'où $\frac{A}{B} = Q + \frac{R}{B}$. $\frac{R}{B}$ ne prend que des valeurs entières ($\frac{A}{B}$ est un cardinal) et tend vers 0 à l'infini en considérant les degrés. Il est donc stationnaire et s'annule ainsi une infinité de fois. D'où $R = 0$.

Recasages possibles (approuvés par Caldéro) : leçons 101, 104, 106, 150, 153, 154, 155, 190.