Prérequis. Décomposition de Fitting.

Théorème 1. *Soient q une puissance d'un nombre premier, $n \geq 1$ et E un $\mathbf{F}_q$-espace vectoriel de dimension n. Alors il y a $\nu_n = q^{n(n-1)}$ endomorphismes de E qui sont nilpotents.*

Démonstration. Définissons pour tout entier n :

- le q-entier $n_q = q^{n-1}(q^n - 1)$;
- la q-factorielle $n!_q = n_q \cdot (n-1)_q \cdot \ldots \cdot 2_q \cdot 1_q$;
- pour tout $k \in \{0, \ldots, n\}$, le q-coefficient binomial $\binom{n}{k}_q = \frac{n!_q}{k!_q (n-k)!_q}$;
- pour toute suite de nombres complexes $a \in \mathbf{C}^{\mathbf{N}}$, la q-série génératrice exponentielle $\Phi_a(x) = \sum_{i \geq 0} a_i \frac{x^i}{i!_q}$.

Soient maintenant $n \geq 1$ et E un $\mathbf{F}_q$-espace vectoriel de dimension n.

Combien y a-t-il de bases de E ? Il y en a :

$$\begin{aligned} |\mathrm{GL}_n(\mathbf{F}_q)| &= (q^n - 1)(q^n - q) \cdot \ldots \cdot (q^n - q^{n-1}) \\ &= (q^n - 1) \cdot q(q^{n-1} - 1) \cdot \ldots \cdot q^{n-1}(q - 1) \\ &= 1_q \cdot 2_q \cdot \ldots \cdot n_q = n!_q. \end{aligned}$$

Combien y a-t-il de décompositions $E = F \oplus G$ avec $\dim(F) = d$? Choisir une telle décomposition revient à choisir une base $(e_1, \ldots, e_n)$ de E et à choisir $F = \langle e_1, \ldots, e_d \rangle$ et $G = \langle e_{d+1}, \ldots, e_n \rangle$ (il y a donc $n!_q$ choix). Cependant il ne faut pas compter plusieurs fois la même décomposition lorsque l'on choisit une autre base de F ou de G, donc il faut diviser le nombre total par $d!_q$ et par $(n-d)!_q$. On obtient alors $\binom{n}{d}_q$ choix.

Posons maintenant $\alpha_n = |\mathrm{Aut}(\mathbf{F}_q^n)|$, $\varepsilon_n = |\mathrm{End}(\mathbf{F}_q^n)|$ et $\nu_n = |\mathrm{Nil}(\mathbf{F}_q^n)|$, définissant trois suites α, ε et ν. On va utiliser leurs q-séries génératrices exponentielles pour obtenir une expression de ν_n.

Calculons Φ_α. D'après la première étape, on a :

$$\Phi_\alpha(x) = \sum_{i \geq 0} |\mathrm{GL}_n(\mathbf{F}_q)| \frac{x^i}{i!_q} = \sum_{i \geq 0} i!_q \frac{x^i}{i!_q} = \sum_{i \geq 0} x^i = \frac{1}{1-x}.$$

Exprimons ε en fonction de α et ν. D'après la décomposition de Fitting, pour chaque $u \in \mathrm{End}(\mathbf{F}_q^n)$ il existe un entier $m \geq 0$ tel que l'on ait la décomposition :

$$E = \mathrm{Ker}(u^m) \oplus \mathrm{Im}(u^m),$$

les deux espaces étant stables par u, la restriction de u sur le noyau étant nilpotente et celle sur l'image étant inversible. Réciproquement, étant donnée une décomposition de la forme $E = F \oplus G$, un endomorphisme nilpotent sur F et un automorphisme de G se recollent en un unique endomorphisme de E. Ainsi, on dispose de la relation :

$$\varepsilon_n = \sum_{i=0}^{n} \binom{n}{i}_q \alpha_i \nu_{n-i},$$

en regroupant les décompositions selon la dimension de G.

Exprimons Φ_ε en fonction de Φ_α et Φ_ν. C'est un simple produit de Cauchy :

$$\begin{aligned}
\Phi_\varepsilon(x) &= \sum_{i=0}^{+\infty} \varepsilon_i \frac{x^i}{i!_q} = \sum_{i=0}^{+\infty} \sum_{j=0}^{i} \binom{i}{j}_q \alpha_j \nu_{i-j} \frac{x^i}{i!_q} \\
&= \sum_{i=0}^{+\infty} \sum_{j=0}^{i} \frac{\alpha_j}{j!_q} x^j \frac{\nu_{i-j}}{(i-j)!_q} x^{i-j} \\
&= \Phi_\alpha(x)\Phi_\nu(x).
\end{aligned}$$

Conclusion. D'après l'expression trouvée précédemment pour Φ_α, on obtient $\Phi_\nu(x) = (1-x)\Phi_\varepsilon(x)$, c'est-à-dire en identifiant les coefficients :

$$\frac{\nu_n}{n!_q} = \frac{\varepsilon_n}{n!_q} - \frac{\varepsilon_{n-1}}{(n-1)!_q}.$$

Autrement dit :

$$\begin{aligned}
\nu_n &= \varepsilon_n - n_q \varepsilon_{n-1} \\
&= q^{n^2} - q^{n-1}(q^n - 1)q^{(n-1)^2} \\
&= q^{n^2} - q^{n+n-1+(n-1)^2} + q^{n-1+(n-1)^2} \\
&= q^{n^2} - q^{2n-1+n^2-2n+1} + q^{n(n-1)} \\
&= q^{n(n-1)}.
\end{aligned}$$

□

Remarques.

- Les séries génératrices sont des séries formelles. Il faut comprendre de quels objets on parle ! Les x écrits ici sont des indéterminées formelles, et tous les calculs sont licites.

- Il faut se rappeler que la décomposition de Fitting vient des noyaux/images itérées. Les suites $\mathrm{Ker}(u^m)$ et $\mathrm{Im}(u^m)$ stationnent à partir du même m par le théorème du rang. Encore avec le théorème du rang, pour montrer la décomposition il suffit de montrer que l'intersection est nulle. Si $x \in \mathrm{Ker}(u^m) \cap \mathrm{Im}(u^m)$ alors en notant $x = u^m(y)$, on a :
$$0 = u^m(x) = u^m(u^m(y)) = u^{2m}(y)$$
donc $y \in \mathrm{Ker}(u^{2m}) = \mathrm{Ker}(u^m)$, d'où $x = 0$. Le fait que les deux espaces soient stables par u et que la restriction au noyau soit nilpotente sont évidents. La resctriction à l'image est un automorphisme car $\mathrm{Im}(u|_{\mathrm{Im}(u^m)}) = u(\mathrm{Im}(u^m)) = \mathrm{Im}(u^{m+1}) = \mathrm{Im}(u^m)$ donc c'est surjectif.

- Il faut aussi absolument savoir expliquer pourquoi le cardinal de $\mathrm{GL}_n(\mathbf{F}_q)$ est $(q^n - 1)(q^n - q) \cdot \ldots \cdot (q^n - q^{n-1})$. Choisir une matrice inversible revient à choisir des vecteurs colonnes qui sont linéairement indépendants dans $\mathbf{F}_q^n$. Ainsi le premier facteur vient du choix du premier vecteur (on peut tout choisir sauf le vecteur nul), le deuxième facteur vient du choix du deuxième vecteur (on peut tout choisir sauf ce qui est dans la droite engendrée par le premier), et ainsi de suite jusqu'à choisir le dernier dans le complémentaire d'un hyperplan.

Recasages.

- 106 : On utilise le cardinal des groupes linéaires sur les corps finis. Attention par contre, les matrices nilpotentes ne sont jamais inversibles, donc il faut que le résultat soit placé au bon endroit. Ce n'est clairement pas la meilleure leçon pour ce développement, ni le meilleur développement pour cette leçon.

- 123 : C'est très bien si l'on fait une partie sur la combinatoire des corps finis par exemple. On pourrait penser à une partie ou une sous-partie qui traite du dénombrement des ensembles de matrices ou des espaces projectifs, et alors ce développement rentre parfaitement. Sinon, ça peut vite glisser hors-sujet.

- 148 : Il faut faire très très attention, la décomposition de Fitting n'est pas une décomposition de matrices au sens usuel du terme. C'est une décomposition de l'espace sur lequel agit la matrice. On peut quand même expliquer que dans une base adaptée à la décomposition de Fitting, la matrice est diagonale par blocs, le premier bloc nilpotent et le second inversible.

- 153 : Si l'on met l'accent sur la justification de la décomposition de Fitting. Mais alors ça devient assez faible, et ça sent le recasage abusif.
- 154 : C'est très bien, encore une fois il faut bien appuyer sur le fait que c'est la décomposition de Fitting qui permet de relier ν à ϵ et α.
- 157 : C'est l'habitat naturel de ce développement.
- 190 : Et ça, c'est sa résidence secondaire.