Thm: Soit $q \in \mathbb{N}$ premier. Alors, la probabilité que 2 éléments de $GL_2(\mathbb{F}_q)$ commutent est $p = \frac{1}{q^2-q}$

Lemme: Soit G un groupe fini, $|G| = n \in \mathbb{N}^*$ et k son nombre de classes de conjugaison. Alors, $p = \frac{k}{n}$ (Admis).

Il faut savoir le montrer !

Dans une leçon sur les corps finis, il faut mettre cette propriété dans le plan

Preuve : . $|GL_2(\mathbb{F}_q)| = \{\text{nb de bases de } \mathbb{F}_q^2\} = (q^2-1)(q^2-q)$ Il faut savoir le montrer !

. Il faut calculer le nb de classes de conjugaison de $G = GL_2(\mathbb{F}_q)$. On, 2 matrices de G sont dans la même classe ssi elles sont semblables. On va donc compter le nombre de classes de similitudes de $M_2(\mathbb{F}_q)$.

par définition

Ainsi, on a 3 cas : les matrices diagonalisables ①, les matrices trigonalisables non diagonalisables ② et les matrices non trigonalisables ③.

cas ①: Soit M diagonalisable. Alors, M est semblable à une matrice de la forme $\text{diag}(\lambda_1, \lambda_2)$, $\lambda_1, \lambda_2 \in \mathbb{F}_q^*$, unique à permutation près.

la matrice doit être inversible.

$|\mathbb{F}_q^*| = q-1$ on a donc $q-1$ choix pour $\lambda_1 = \lambda_2$ et $\binom{q-1}{2}$ pour $\lambda_1 \neq \lambda_2$, ce qui nous donne $\frac{(q-1)q}{2}$ classes de matrices diagonalisables.

$\binom{q-1}{2} = \frac{(q-1)!}{(q-3)!2!} = \frac{(q-1)(q-2)}{2}$ $\qquad \frac{(q-1)(q-2)}{2} + (q-1) = \frac{(q-1)q}{2}$

cas ②: Soit $\epsilon = \mathbb{F}_q^2$. Soit $u \in \mathcal{L}(\epsilon)$ trigonalisable non diagonalisable. χ_u est donc scindé sur $\mathbb{F}_q$ mais pas scindé simple. De plus, si non elle serait diagonalisable

$\deg(\chi_u) = 2 \Rightarrow \chi_u$ de la forme $(X-\lambda)^2$, $\lambda \in \mathbb{F}_q^*$. Par hypothèse, $\exists (e_1, e_2)$ base de ϵ tq $\text{mat}_{(e_1,e_2)}(u) = \begin{pmatrix} \lambda & \varepsilon \\ 0 & \lambda \end{pmatrix}$, $\varepsilon \in \mathbb{F}_q^*$.

Donc, dans la base $(e_1', e_2') = (e_1, \frac{e_2}{\varepsilon})$, on a $\text{mat}_{(e_1', e_2')}(u) = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. Ainsi, il y a autant de classes de similitudes que de λ dans $\mathbb{F}_q^*$, càd $q-1$.

cas ③: Soit $f \in \mathcal{L}(\epsilon)$ non trigonalisable. χ_f est non scindé sur $\mathbb{F}_q$ et de degré 2, donc sans racine. On, il y a q^2 polynômes unitaires de degré 2 dans $\mathbb{F}_q[X]$. Il faut donc retirer les polynômes de la forme $(X-\lambda)^2$ et $(X-\lambda_1)(X-\lambda_2)$ à permutation près

$X^2 + aX + b$ avec $a, b \in [\![1, q]\!]$ → $q \times q = q^2$ choix.

(car $\mathbb{F}_q[X]$ factoriel). Ainsi, on a $q^2 - q - \binom{q}{2} = q^2 - q - \frac{q(q-1)}{2} = \frac{q(q-1)}{2}$ polynômes sans racine de degré 2 dans $\mathbb{F}_q$. On va maq chacun de ces polynômes détermine une classe de conjugaison. On pose $P = \chi_f = X^2 - aX - b \in \mathbb{F}_q[X]$ sans racine et soit e_1 vecteur non nul de E.

$P(f) = 0$

On va expliciter une matrice de f.

on met des $-$ pour se faciliter la vie après.

$f(e_1) \neq \lambda e_1$ $\forall \lambda \in \mathbb{F}_q$ (sinon λ serait vp de f et donc racine de $P \rightarrow$ Absurde) donc $(e_1, f(e_1))$ base de ϵ. Posons $e_2 = f(e_1)$, par Cayley-Hamilton :

$f(e_2) = f^2(e_1) = (af + b\text{Id})(e_1) = ae_2 + be_1$. Ainsi, $\text{mat}_{(e_1,e_2)}(f) = \begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix}$ et cette matrice ne dépend que de P. Donc [illegible] autant de

matrices inversibles non trigonalisables que de polynôme de degré 2 sans racine dans $\mathbb{F}_q[X]$. (0 pas racine de $P \Leftrightarrow P(0) \neq 0 \Leftrightarrow \det(P) \neq 0$)

Il y a donc $\frac{q(q-1)}{2}$ classes de conjugaison.

Au final, dans G, on trouve $h = \frac{q^2-q}{2} + q - 1 + \frac{q(q-1)}{2} = \frac{q^2-q+2q-2+q^2-q}{2} = \frac{2q^2-2}{2} = q^2-1$ et enfin $p = \frac{q^2-1}{(q^2-1)(q^2-q)} = \frac{1}{q^2-q}$. □

Référence: Carnet de voyage en Analysbon, Philippe Caldero (exercice 108)

Je la mets dans ces leçons, mais pas en dev, juste en application.

Leçons: 101 - 103 - 104 - 106 - 190 - 123 - 150 - 156

OK — possible — mitigé car le niveau du développement sur ces leçons n'est peut-être pas assez poussé, mais rien de catégorique.

Les commentaires sous les leçons proviennent d'un prof à qui j'ai demandé de l'aide pour les recasages

Remarques:

- Pour choisir ce dev, il faut savoir démontrer Burnside, le lemme et $|GL_2(\mathbb{F}_q)| = (q^2-1)(q^2-q)$.
- Dans la référence, on fait pour $q=5$: la méthode est identique pour $q \in \mathbb{N}^*$ premier.
- Si dev trop court, on peut démontrer le lemme en 2 minutes.

$|GL_2(\mathbb{F}_q)| = (q^2-q)(q^2-1)$

Preuve: Un élément de $GL_2(\mathbb{F}_q)$ peut être vu comme un couple de 2 vecteurs indépendants d'un $\mathbb{F}_q$-ev de dim 2.

Pour choisir le premier vecteur, il y a donc q^2-1 possibilités (on veut juste un vecteur non nul). Pour le choix du second vecteur, on veut juste qu'il ne soit pas colinéaire au premier. Or, on est dans $\mathbb{F}_q$ donc il y a q vecteurs colinéaires au premier et donc q^2-q vecteurs possibles. Ainsi, $|GL_2(\mathbb{F}_q)| = (q^2-1)(q^2-q)$. □

Preuve Lemme: Ici, le nb de classes de conjugaison est égal au nb d'orbites pour l'action de G sur G. Soit K l'ensemble des couples d'éléments de G qui commutent, alors $p = \frac{|K|}{m^2}$. Par définition, $K \overset{(1)}{=} \bigcup_{g \in G} \{g\} \times Fix(g) \Rightarrow |K| = \sum_{g \in G} |Fix(g)|$.

Ainsi, par la Formule de Burnside, $h_2 = \frac{1}{m}|K| = \frac{1}{m} p m^2 = pm \Rightarrow p = \frac{h}{m}$. □

(1) $\Leftrightarrow \forall g \in G, Fix(g) = \{h \in G \mid ghg^{-1} = h\} = \{h \in G \mid$ [illegible] $\}$

Donc, $K = \bigcup_{g \in G} \{g\} \times Fix(g) \Rightarrow |K| = \sum_{g \in G} |Fix(g)|$

Burnside: Soit G un groupe fini et X un ensemble fini. On note $|\Omega|$ le nombre d'orbite pour l'action de G sur X. Alors,

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|.$$

Preuve: Soit $C = \{(g,x) \mid g \in G, x \in X\}$. On calcule $|C|$ de 2 façons:

- $C = \bigcup_{g \in G} \{g\} \times Fix(g) \Rightarrow |C| = \sum_{g \in G} |Fix(g)|$

- $C = \bigcup_{x \in X} Stab(x) \times \{x\} \Rightarrow |C| = \sum_{x \in X} |Stab(x)| = \sum_{x \in X} \frac{|G|}{|O_x|}$. De plus, les orbites sont des classes d'équivalence, donc les orbites partitionnent X.

$|O_x|$: orbite de x

$x \sim y \Leftrightarrow \exists g \in G$ tq $y = g \cdot x$

Ainsi, soit $\omega \in \Omega$, $\forall x \in \omega$, $O_x = \omega$ et $|C| = \sum_{\omega \in \Omega} \sum_{x \in \omega} \frac{|G|}{|\omega|} = \sum_{\omega \in \Omega} |G| = |\Omega||G|$.

Enfin, $|\Omega| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$. □