Dév : Corps finis et Dobble.

Recasages :
- 109 : Formes linéaires, hyperplans, dualité.
- 307 : Exercices faisant intervenir des dénombrements.
- 357 : Exercices utilisant le corps $\mathbb{Z}/p\mathbb{Z}$.

Source(s) :
- Skandalis, ex. 5.14 p. 162

$(\mathbb{F}_p^n = (\mathbb{Z}/p\mathbb{Z})^n)$.

Énoncé : Soient $p \in \mathbb{P}$ et $n \in \mathbb{N}^*$, et $k \in [\![0;n]\!]$.

1. Combien y a-t-il de droites dans l'espace vectoriel $\mathbb{F}_p^n$? Et combien d'hyperplans ?
2. Combien y a-t-il de systèmes libres à k éléments dans $\mathbb{F}_p^n$? Et combien de bases ?
3. Combien y a-t-il de sous-espaces vectoriels de dimension k dans $\mathbb{F}_p^n$?
4. Le jeu de Dobble consiste en 57 cartes, chacune comportant 8 symboles. Chaque couple de cartes a un unique symbole en commun. Proposer un moyen de construction d'un tel jeu.

1 • Nombre de droites dans $\mathbb{F}_p^n$:

* $p^n - 1$ éléments non nuls dans $\mathbb{F}_p^n$, et chaque élément appartient à une unique droite.
* Chaque droite contient $p-1$ éléments non nuls
  ↳ en effet, pour être dans la même droite, je multiplie mon vecteur par un élément de $\mathbb{F}_p$ non nul. Or il y en a $p-1$.

$\Rightarrow$ Il y a $\boxed{\frac{p^n-1}{p-1} \text{ droites}}$ dans $\mathbb{F}_p^n$.

• Nombre d'hyperplans dans $\mathbb{F}_p^n$:

Rappels :
* E un $\mathbb{K}$-ev. On appelle forme linéaire sur E une application linéaire de E à valeurs dans $\mathbb{K}$.
* Le dual de E (noté E^*) est l'espace $\mathcal{L}(E,\mathbb{K})$ des formes linéaires sur E.
* Un hyperplan de E est un sev H qui vérifie :
  $\exists e \in E$ non nul tel que $E = \mathbb{K}e \oplus H$.
  $\Leftrightarrow E \neq H$ et $\forall e \in E \setminus H$, $E = \mathbb{K}e \oplus H$.
  $\Leftrightarrow \exists f \in E^*$ non nulle telle que $H = \ker(f)$.

* $d \longmapsto d^\perp$ est une bijection de l'ensemble des droites de $\mathbb{F}_p^n$ sur l'ensemble des hyperplans de son dual $(\mathbb{F}_p^n)^*$.

Donc il y a $\frac{p^n-1}{p-1}$ hyperplans dans $(\mathbb{F}_p^n)^*$.

Or $\mathbb{F}_p^n$ et $(\mathbb{F}_p^n)^*$ sont isomorphes, donc ils ont autant d'hyperplans.

$\Rightarrow$ Il y a $\boxed{\frac{p^n-1}{p-1} \text{ hyperplans}}$ dans $\mathbb{F}_p^n$.

2 • Nombre de systèmes libres à k éléments :

* 1^{er} vecteur non nul : $p^n - 1$ choix
* $2^{ème}$ vecteur non colinéaire au premier : $p^n - p$ choix

⋮

* Quand on a choisi j vecteurs, ils engendrent un espace de dimension j qui contient p^j éléments, donc pour le $j+1$-ème, on a $p^n - p^j$ choix.

$\Rightarrow$ $\boxed{(p^n-1)(p^n-p)\cdots(p^n-p^{k-1}) \text{ systèmes libres à } k \text{ éléments}}$ dans $\mathbb{F}_p^n$.

• Nombre de bases :

Les bases de $\mathbb{F}_p^n$ ont n éléments, d'où :

$\Rightarrow$ Il y a $\boxed{(p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) \text{ bases}}$ dans $\mathbb{F}_p^n$.

3 Nombre de s.e.v. de dimension k :

On note : $\begin{cases} L_k : \text{ensemble des familles libres à } k \text{ éléments.} \\ G_k : \text{ensemble des sous-e.v. de dimension } k. \end{cases}$

Soit $\varphi : L_k \longrightarrow G_k$
$\ell \longmapsto \mathrm{Vect}(\ell)$, ℓ est une base de $\mathrm{Vect}(\ell)$

$\forall F \in G_k$, F admet une base qui appartient donc à L_k, donc φ est surjective.

Donc $\varphi^{-1}(F)$ est l'ensemble des bases de F.

Or un élément de G_k est un ss-e.v. de dimension k, qui a donc $(p^k-1)(p^k-p)\cdots(p^k-p^{k-1})$ bases d'après 2. On a aussi que L_k contient $(p^n-1)(p^n-p)\cdots(p^n-p^{k-1})$ éléments.

G_k admet donc :

$$\frac{(p^n-1)(p^n-p)\cdots(p^n-p^{k-1})}{(p^k-1)(p^k-p)\cdots(p^k-p^{k-1})} = \frac{(p^n-1)\cdot \cancel{p}(p^{n-1}-1)\cdots \cancel{p^{k-1}}(p^{n-k+1}-1)}{(p^k-1)\cdot\cancel{p}(p^{k-1}-1)\cdots\cancel{p^{k-1}}(p-1)}$$

$$= \boxed{\frac{(p^n-1)(p^{n-1}-1)\cdots(p^{n-k+1}-1)}{(p^k-1)(p^{k-1}-1)\cdots(p-1)}} \text{ éléments.}$$

4 Jeu de Dobble :

Dans $\mathbb{F}_p^3$, il y a $\frac{p^3-1}{p-1} = \frac{\cancel{(p-1)}(p^2+p+1)}{\cancel{p-1}} = p^2+p+1$ droites et plans ; et chaque plan contient $p+1$ droites. Deux droites distinctes sont contenues dans un seul plan commun.

Soit f une bijection entre : $(p=7)$

- l'ensemble des $7^2+7+1=57$ cartes.
- l'ensemble des droites de $\mathbb{F}_7^3$.

Soit g une bijection entre :

- l'ensemble des 57 symboles.
- l'ensemble des plans de $\mathbb{F}_7^3$.
  - chaque plan contient $7+1=8$ droites.

On pose que :

- La carte y contient le symbole x si le plan $g(y)$ contient la droite $f(x)$.

Alors on aura bien que chaque carte contient 8 symboles, et que 2 cartes ont un seul symbole commun.

Rmq : Dans le vrai jeu de Dobble, il n'y a en fait que 55 cartes, 2 ont été oubliées/retirées.

Rmq : Il y a d'autres façons de construire le jeu, notamment avec des plans de fano (plan projectif minimal), voir la super vidéo de Matt Parker (sur la chaîne YouTube Stand-up Maths) à ce sujet !