Dossier de synthèse de TIPE :

Espaces projectifs, corps finis et jeux de cartes

Cyprien MANGEOT - Eugénie ROGER

L3 Mathématiques & Applications 2020-2021

Table des matières

Édité par Asmodée en 2009, Dobble est un jeu de société relativement connu et amusant. Il est constitué de 55 cartes rondes possédant chacune 8 symboles. S'il existe plusieurs variantes, le but du jeu est toujours de trouver le symbole en commun entre deux cartes données.
La propriété remarquable du jeu de Dobble est que chaque carte possède un unique symbole commun avec toute autre carte du paquet. Ainsi, il est toujours possible de trouver un symbole commun entre deux cartes, et il n'y a jamais deux symboles communs entre deux cartes. Si cela peut paraître impressionnant à première vue, Dobble est en fait basé sur une structure mathématique empruntée à la géométrie finie.

1 Corps finis

1.1 Rappels sur les anneaux

Définition 1.1. Un **anneau** est un ensemble A muni de deux lois de compositions internes : une addition et un produit.
On dit que $(A, +, \times)$ est un anneau si :

- $(A, +)$ est un groupe commutatif.
- le produit est associatif.
- le produit est distributif par rapport à l'addition, c'est-à-dire :
  $\forall x, x', y, y' \in A$,
  - $(x + x')y = xy + x'y$
  - $x(y + y') = xy + xy'$

  où pour tout $x, y \in A$ on note xy pour $x \times y$.

On dit que $(A, +, \times)$ est un anneau *commutatif* si le produit est commutatif.
L'élément neutre pour $(A, +)$ est noté 0_A. Si le produit admet un élément neutre, celui-ci est noté 1_A et on dit que l'anneau $(A, +, \times)$ est *unitaire.*

Définition 1.2. Soit A un anneau commutatif. Un **idéal** de A est un sous-groupe I de $(A, +)$ tel que :

$$\forall a \in A,\ \forall x \in I,\ ax \in I.$$

Exemple 1.3. Soit $n \in \mathbb{N}$.

- L'anneau $\mathbb{Z}$ muni de l'addition et de la multiplication est commutatif. Les ensembles $n\mathbb{Z}$ sont les idéaux de $\mathbb{Z}$.
- $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence, notées $\overline{k}$ avec $k \in \{0, 1, \ldots, n-1\}$, pour la relation de *congruence modulo n*.
- $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ muni de l'addition et de la multiplication *modulo* n est un anneau commutatif.

Définition 1.4. Soit $(A, +, \times)$ un anneau commutatif. A est dit **intègre** si :

$$(\forall x, y \in A,\ xy = 0) \Longleftrightarrow (x = 0 \textit{ ou } y = 0)$$

Définition 1.5. — Un **corps** est un anneau K unitaire (d'élément neutre $1_K \neq 0_K$) dans lequel tout élément non nul x possède un inverse x^{-1}.
— Si le produit est commutatif, on dira que le corps K est un **corps commutatif**.
— Un **corps fini** est un corps commutatif qui possède un nombre fini d'éléments.

Théorème 1.6. *Soit $n \in \mathbb{N}^*$. Alors les assertions suivantes sont équivalentes :*
1. *n est premier*
2. *$\mathbb{Z}/n\mathbb{Z}$ est intègre*
3. *$\mathbb{Z}/n\mathbb{Z}$ est un corps*

Démonstration. $1 \Rightarrow 3$: Soit $\overline{x} \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$. Alors n ne divise pas x et comme n est premier, $x \wedge n = 1$ donc $\overline{x}$ est inversible, donc $\mathbb{Z}/n\mathbb{Z}$ est un corps.
$3 \Rightarrow 2$: Soient $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$ tels que $\overline{x}\ \overline{y} = \overline{0}$. Si $\overline{y} \neq \overline{0}$, alors $\overline{y}$ est inversible, donc $\overline{x} = \overline{x}\ \overline{y}\ \overline{y}^{-1} = \overline{0}\ \overline{y^{-1}} = \overline{0}$ donc $\mathbb{Z}/n\mathbb{Z}$ est intègre.
$2 \Rightarrow 1$: Soient $n_1, n_2 \in \mathbb{N}_{\geq 2}$, où $n = n_1 n_2$. On a $\overline{n} = \overline{n_1}\ \overline{n_2} = \overline{0}$ et $\overline{n_1}, \overline{n_2} \neq \overline{0}$, donc si n n'est pas premier alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. On en déduit que si $\mathbb{Z}/n\mathbb{Z}$ est intègre alors n est premier. □

Définition 1.7. Soit A un anneau unitaire (d'élément neutre 1_A). L'application :

$$f : \begin{array}{ccc} \mathbb{Z} & \to & A \\ n & \mapsto & n \times 1_A \end{array}$$

est un homomorphisme d'anneaux. Son noyau est un idéal de $\mathbb{Z}$ donc $Ker(f) = p\mathbb{Z}$, où p est un entier positif appelé **caractéristique** de A.

Proposition 1.8. Un corps fini est déterminé à isomorphisme près par son cardinal, qui est toujours une puissance d'un nombre premier. Ce nombre premier est la caractéristique du corps. Ainsi pour tout nombre premier p et pour tout $n \in \mathbb{N}^*$, il existe un corps de cardinal p^n. Celui-ci est isomorphe au corps $(\mathbb{Z}/p\mathbb{Z})^n$.

Remarque 1.9. Le corps fini de cardinal q, où q est une puissance d'un nombre premier, est noté $\mathbb{F}_q$.

1.2 Le corps $\mathbb{F}_p$

Soit p un nombre premier. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$. D'après le théorème 1.6, $\mathbb{F}_p$ est un corps.

Proposition 1.10. Soit $\mathbb{F}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$ muni de l'addition et de la multiplication *modulo p*. Alors :
— Chaque élément $\overline{x}$ de $\mathbb{F}_p$ a un unique opposé noté $-\overline{x}$.
— Chaque élément non nul $\overline{x}$ de $\mathbb{F}_p$ a un unique inverse noté $\overline{x}^{-1}$.

Exemple 1.11. Soit $p = 2$. On considère $\mathbb{F}_2$ muni de l'addition et de la multiplication *modulo* 2.

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Figure 1 – Tables d'addition et de multiplication de $\mathbb{F}_2$

On remarque que $\overline{0}$ (resp. $\overline{1}$) possède un unique opposé dans $\mathbb{F}_2$: $\overline{0}$ (resp. $\overline{1}$). De plus, $\overline{1}$ possède un unique inverse dans $\mathbb{F}_2$: lui-même.

Exemple 1.12. On considère $p = 7$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Figure 2 – Tables d'addition et de multiplication de $\mathbb{F}_7$

On peut ainsi vérifier que chaque élément de $\mathbb{F}_7$ possède un unique opposé et que chaque élément non nul de $\mathbb{F}_7$ possède un unique inverse :

$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$-\overline{x}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\overline{x}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{x}^{-1}$	$\overline{1}$	$\overline{4}$	$\overline{5}$	$\overline{2}$	$\overline{3}$	$\overline{6}$

Figure 3 – Tables des opposés et des inverses dans $\mathbb{F}_7$

2 Espaces projectifs

2.1 Premières définitions

Dans cette section, K désigne un corps.

Définition 2.1. Soit E un K-espace vectoriel. La **relation de colinéarité** $\mathcal{R}$ est la relation d'équivalence définie pour tout $x, y \in E \setminus \{0\}$ par :

$$x\mathcal{R}y \iff \exists\lambda \in K^*,\ y = \lambda x.$$

Définition 2.2. Soit E un K-espace vectoriel. L'**espace projectif associé à** E, noté $P(E)$, est l'ensemble quotient de $E \setminus \{0\}$ par la relation de colinéarité $\mathcal{R}$:

$$P(E) \simeq (E \setminus \{0\})/_{\mathcal{R}}.$$

Autrement dit, c'est l'ensemble des droites vectorielles de E, à l'exclusion du vecteur nul.

Proposition 2.3. Soit $n \in \mathbb{N}_{\geq 2}$. Si E est un K-espace vectoriel de dimension finie n, alors $P(E)$ est de dimension finie $n-1$:

$$\mathbf{dim}(P(E)) \;=\; \mathbf{dim}(E)\; -1.$$

Remarque 2.4. — On parle de *droite projective* (respectivement *plan projectif*) si l'espace projectif $P(E)$ est de dimension 1 (respectivement de dimension 2).

— On note $P_n(\mathbb{R})$ l'espace projectif réel de dimension n.

2.2 Plans projectifs

Définition 2.5. Une **structure d'incidence** est un triplet $(\Omega, \Delta, \mathcal{I})$ où :

— Ω est un ensemble de points.

— Δ est un ensemble de droites, où $\Delta \subset \mathcal{P}(\Omega)$.

— $\mathcal{I}$ est une relation dite *d'incidence* entre les points de Ω et les droites de Δ.
On dit que $A \in \Omega$ est **incident** à $d \in \Delta$ si, et seulement si, $A \in d$ (c'est-à-dire « la droite d passe par le point A », ou encore « le point A est sur la droite d »).

Définition 2.6. Soit $n \in \mathbb{N}_{\geq 3}$.

— Si n points de Ω sont incidents à une même droite $d \in \Delta$, on dit que ces points sont **alignés** sur d.

— Si un point $A \in \Omega$ est incident à n droites distinctes de Δ, on dit que ces droites sont **concourantes** en A.

— On dit que deux droites distinctes d_1 et d_2 **se coupent** en un point A si A est incident à d_1 et d_2.

Proposition et définition 2.7. Un **plan projectif** est une structure d'incidence vérifiant les axiomes d'incidence suivants :

- **(A1) :** Par deux points distincts passe une unique droite.
- **(A2) :** Deux droites distinctes se coupent en un unique point.
- **(A3) :** Chaque droite passe par au moins trois points.
- **(A4) :** Il existe au moins trois points non alignés.

Remarque 2.8. — L'axiome (A1) est toujours vérifié en géométrie affine et projective, même en dimension infinie.

— L'axiome (A2) nous garantit que toutes les droites sont dans un même plan et qu'il n'existe pas de droites parallèles.

— Les axiomes (A3) et (A4) nous permettent d'avoir un nombre suffisant de points afin d'éliminer les cas triviaux qui ne peuvent être considérés comme des plans projectifs. Par exemple, l'axiome (A4) nous assure que la structure étudiée n'est pas réduite à une seule droite.

Proposition 2.9 (Quadrangle complet)**.** On peut remplacer les deux axiomes (A3) et (A4) par l'axiome suivant :

- **(A) :** Il existe au moins 4 points trois à trois non alignés.

Une telle configuration de 4 points définit 6 droites distinctes et est appelée *quadrangle complet.*

Démonstration. ($\Rightarrow$) On suppose (A3) et (A4).
D'après (A4), il existe trois points A, B et D non alignés. D'après (A1), ces points définissent deux droites distinctes (AB) et (AD). D'après (A3), la droite (AB) passe par un point E distinct de A et B, et la droite (AD) passe par un point F distinct de A et D. Les points B et F sont distincts car F appartient à la droite (AD) et A est l'unique point d'intersection de (AB) et (AD). De même, les points D et E sont distincts. D'après (A1), on peut donc définir les droites (BF) et (DE), qui sont distinctes car leurs points d'intersection respectifs avec (AB) sont distincts. En effet, $(BF) \cap (AB) =$ B et $(DE) \cap (AB) =$ E, avec B et E distincts. D'après (A2), les droites (BF) et (DE) se coupent en un unique point C. Ainsi :

- Les points A, B et D sont non alignés.
- Si les points A, B et C (resp. A, B et D) sont alignés, alors C est sur la droite (AB) (resp. (AD)). Comme C est sur (BF) (resp. (DE)), alors F (resp. E) est sur (AB) et sur (AD) donc les droites (AB) et (AD) sont confondues, ce qui est absurde car les points A, B et D ne sont pas alignés. Ainsi les points A, B et C (resp. A, C et D) ne sont pas alignés.
- Si les points B, C et D sont alignés, alors les droites (BC) et (CD) sont confondues. Comme F est sur (BC) et E est sur (CD), alors les droites (BF) et (DE) sont confondues, ce qui est absurde car ces droites sont distinctes et se coupent en un unique point.

On en déduit que les A, B, C et D sont trois à trois non alignés. Ainsi l'axiome (A) est vérifié.

($\Leftarrow$) Supposons (A). Alors il existe 4 points A, B, C et D 3 à 3 non alignés.
L'axiome (A4) est trivialement vérifié.
Comme A, B, C et D sont 3 à 3 non alignés, alors les droites (AB) et (CD) sont distinctes. D'après (A2), on peut définir E $= (AB) \cap (CD)$.
De même, les droites (BC) et (AD) sont distinctes. Grâce à (A2), on peut donc définir F $= (BC) \cap (AD)$. Cela implique que chaque droite contient bien au moins 3 points. Ainsi L'axiome (A3) est aussi vérifié. $\square$

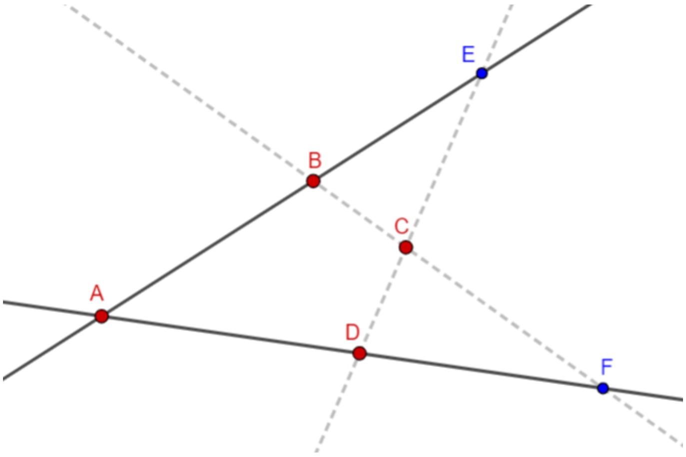

FIGURE 4 – Exemple de quadrangle complet

Proposition 2.10 (Axiome de Desargues)**.** Soient ABC et A'B'C' deux triangles non plats dont les sommets sont sur trois droites (AA'), (BB') et (CC') distinctes et concourantes. Alors les points P $:= (BC) \cap (B'C')$, Q $:= (AC) \cap (A'C')$ et R $:= (AB) \cap (A'B')$ sont alignés.

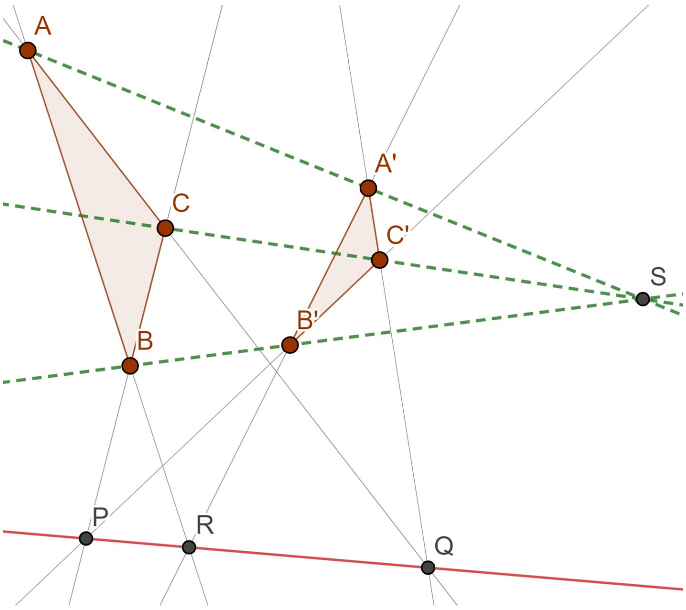

FIGURE 5 – Illustration de l'axiome de Desargues dans le plan projectif réel

Définition 2.11. Un plan projectif est dit **arguésien** s'il satisfait l'axiome de Desargues. À l'inverse, un plan projectif est dit **non arguésien** s'il ne vérifie pas cet axiome.

Remarque 2.12. Dans un espace projectif de dimension supérieure ou égale à 3, l'axiome de Desargues est toujours vérifié. Ainsi un plan projectif est un plan d'un espace projectif de dimension supérieure ou égale à 3 si, et seulement si, il satisfait l'axiome de Desargues.

Proposition 2.13 (Axiome de Pappus)**.** Soient (A,B,C) et (A',B',C') deux triplets de points alignés distincts. Alors les points P $:= (B'C) \cap (BC')$, Q $:= (A'C) \cap (AC')$ et R $:= (A'B) \cap (AB')$ sont alignés.

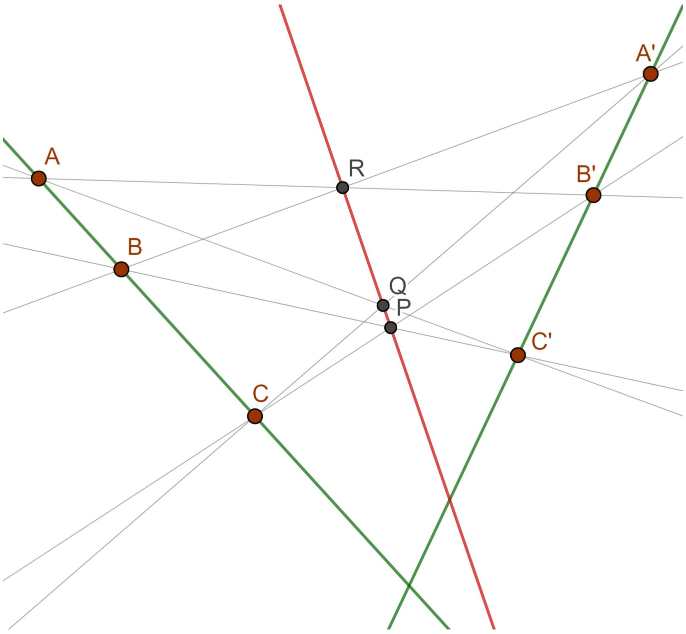

Figure 6 – Illustration de l'axiome de Pappus dans le plan projectif réel

Théorème 2.14 (Théorème de Hessenberg)**.** *Si un plan projectif vérifie l'axiome de Pappus, alors il vérifie également l'axiome de Desargues.*

Démonstration. Soient ABC et A'B'C' deux triangles non plats dont les sommets sont sur trois droites (AA'), (BB') et (CC') distinctes et concourantes en un point S.
On considère les points P $:= (BC) \cap (B'C')$, Q $:= (AC) \cap (A'C')$ et R $:= (AB) \cap (A'B')$.

— Soit D $:= (AC) \cap (B'C')$. On applique l'axiome de Pappus aux triplets de points alignés (S,B',B) et (A,C,D) : les points $(AB) \cap (SD) =:$ E, $(AB') \cap (SC) =:$ F et $(BC) \cap (B'D) = (BC) \cap (B'((AC) \cap (B'C'))) = (BC) \cap (B'C') =$ P sont alignés. Autrement dit, P appartient à la droite (EF) et on peut écrire P $= (EF) \cap (B'D)$.

— On applique l'axiome de Pappus aux deux triplets de points alignés (S,A,A') et (B',C',D) : les points $(AB') \cap (SC') = (AB') \cap (SC) =$ F, $(AB') \cap (SD) =:$ G et $(A'C') \cap (AD) = (A'C') \cap (A((AC) \cap (B'C'))) = (A'C') \cap (AC) =$ Q sont alignés. Autrement dit, Q appartient à la droite (FG) et on peut écrire Q $= (FG) \cap (AC)$.

— On applique une dernière fois l'axiome de Pappus aux triplets de points alignés (A,B',F) et (G,E,D) : les points $(EF) \cap (B'D) =$ P, $(FG) \cap (AD)$ et $(B'G) \cap (AE)$ sont alignés. Or on a :

  - $(FG) \cap (AD) = (FG) \cap (A((AC) \cap (B'C'))) = (FG) \cap (AC) = Q$
  - $(B'G) \cap (AE) = (B'((A'B') \cap (SD))) \cap (A((AB) \cap (SD))) = (A'B') \cap (AB) = R$

On en déduit que les points P, Q et R sont alignés donc l'axiome de Desargues est vérifié. □

2.3 Construction à partir du plan affine

On peut également définir le plan projectif à partir du plan affine.

Proposition et définition 2.15. Un **plan affine** est une structure d'incidence vérifiant les axiomes d'incidence suivants :

- **(B1) :** Par deux points distincts passe une unique droite.
- **(B2) :** Il existe au moins trois points non alignés.
- **(B3) :** Pour tout point A et toute droite d ne passant pas par A, il existe une unique droite d' passant par A telle que d et d' soient disjointes.

Remarque 2.16. Les axiomes (B1) et (B2) du plan affine correspondent respectivement aux axiomes (A1) et (A4) du plan projectif.

On considère une structure d'incidence qui satisfait les axiomes d'incidence du plan affine. Pour obtenir une structure d'incidence qui satisfait les axiomes d'incidence du plan projectif, on ajoute un point dit *point à l'infini* pour chaque direction de droite, et une droite dite *droite à l'infini* qui passe par tous les points à l'infini, de sorte que :

- un point à l'infini est incident à toutes les droites d'une même direction
- un point à l'infini est incident à la droite à l'infini

Exemple 2.17. *Construction du plan projectif réel.*
On considère le plan affine réel constitué de tous les points (x, y) où $x, y \in \mathbb{R}$ et de toutes les droites passant par ces points.
On construit le plan projectif réel à partir du plan affine réel en y ajoutant un nouveau point pour chaque direction de droite : le *point à l'infini* de cette direction.
Ainsi deux droites parallèles, qui ont donc la même direction, définissent le même point à l'infini.
Dans le plan affine réel, deux droites parallèles ne se coupent pas, tandis que dans le plan projectif réel, deux droites parallèles se coupent en un unique point : le point à infini associé à leur direction. Si plusieurs droites sont parallèles entres elles, elles sont concourantes en un même point : le point à l'infini associé à leur direction.
Les droites du plan projectif réel sont celles du plan affine réel auxquelles on a ajouté les points à l'infini (définis par leurs directions respectives). On ajoute également la droite constituée de l'ensemble des points à l'infini : la *droite à l'infini*. On note $\mathcal{P}_2(\mathbb{R})$ le plan projectif réel que l'on vient de définir.

Remarque 2.18. Les plans projectifs construits à partir des plans affines complétés par les points et la droite *à l'infini* sont équivalents à ceux construits de manière axiomatique si et seulement si ils sont arguésiens.

3 Espaces projectifs sur les corps finis

3.1 Premières propriétés

Proposition et définition 3.1. Soit $n \in \mathbb{N}_{\geq 2}$. Un **plan projectif fini** d'ordre n est une structure d'incidence munie des axiomes d'incidence suivants :

- **(A1) :** Par deux points distincts passe une unique droite.
- **(A2) :** Deux droites distinctes se coupent en un unique point.
- **(A3') :** Chaque droite passe par $n+1$ points distincts.
- **(A4') :** Par chaque point passent $n+1$ droites distinctes.

Remarque 3.2. Ici, il faut bien considérer une droite comme l'ensemble des points qui lui sont incidents, et non comme une infinité de points.

Proposition 3.3. Un plan projectif fini d'ordre n possède n^2+n+1 points et autant de droites.

Démonstration. On considère un plan projectif fini d'ordre n. Soit A un point de ce plan.
D'après (A4'), il y a $n+1$ droites qui passent par A. D'après (A3'), chacune de ces droites passe par $n+1$ points, donc par A et n points deux à deux distincts (et distincts de A). Ainsi le plan projectif considéré possède $1+n(n+1)$ points (le point A ainsi que n points sur chacune des $n+1$ droites qui passent par A).
De même, étant donnée une droite d, le plan considéré possède $1+n(n+1)$ droites (la droite d ainsi que n droites passant par chacun des $n+1$ points de d). $\square$

Proposition 3.4. S'il existe un corps fini de cardinal q, alors il existe un plan projectif d'ordre q.

Comme il existe un corps fini de cardinal q si et seulement si q peut s'écrire comme puissance d'un nombre premier, on en déduit le théorème :

Théorème 3.5. *Si q peut s'écrire comme puissance d'un nombre premier, alors il existe un plan projectif d'ordre q.*

Théorème 3.6 (Théorème de Bruck-Ryser)**.** *S'il existe un plan projectif d'ordre $q \equiv 1 \pmod 4$ ou $q \equiv 2 \pmod 4$, alors q est la somme de deux carrés (éventuellement nuls).*

Remarque 3.7.

- Le théorème de Bruck-Ryser nous dit que tous les entiers $n \in \mathbb{N}$ tels que $n \equiv 1, 2 \pmod 4$ qui ne sont pas somme de deux carrés, ne peuvent pas être les ordres d'un plan projectif.
- Les ordres $q_1 = 5 = 2^2+1^2$, $q_2 = 9 = 3^2+0^2$ et $q_3 = 13 = 3^2+2^2$ satisfont les conditions du théorème de Bruck-Ryser, ils peuvent donc être des ordres de plans projectifs.
- On sait par ailleurs que toutes les puissances de nombre premier peuvent être l'ordre d'un plan projectif. Que peut-on dire des entiers restants ? C'est-à-dire, les entiers n'étant dans aucune de ces deux catégories.
  En fait, on ne peut rien dire concernant ces entiers.

Remarque 3.8. La liste des entiers n tels que $n \equiv 1, 2 \pmod 4$ qui ne sont pas somme de deux carrés est disponible sur le site de l'OEIS (On-Line Encyclopedia of Integer Sequences).

Exemple 3.9.
— Pour $n = 10$, on constate que n n'est pas puissance d'un nombre premier, et n ne satisfait pas les conditions du théorème de Bruck-Ryser.
On ne peut donc a priori rien dire sur l'existence d'un plan projectif d'ordre 10.
Mais en 1989, Christian LAM a prouvé l'impossibilité pour l'ordre 10 par analyse exhaustive à l'aide d'un ordinateur.
— Pour $n = 12$, la question de l'existence ou non d'un plan projectif d'ordre 12 est toujours ouverte.

Remarque 3.10. Tous les plans projectifs finis connus ont pour ordre une puissance de nombre premier.

3.2 Le plan de Fano

En géométrie projective finie, le *plan de Fano*, qui tient son nom du mathématicien italien Gino Fano, est le plus petit plan projectif fini. C'est aussi le plan projectif sur le corps fini à deux éléments $\mathbb{F}_2$: on le note $P_2(\mathbb{F}_2)$. Il est le seul à posséder 7 points et 7 droites et vérifie donc la proposition 3.3 en tant que plan projectif fini d'ordre 2 : en effet, $2^2 + 2 + 1 = 7$.

Définition 3.11. Soit D une droite non verticale. On peut calculer la **pente** t de la droite D de la manière suivante :
Soit $A = (x_a, y_a)$ et $B = (x_b, y_b)$ deux points se trouvant sur la droite D.
La pente t est alors donnée par $t = \frac{y_b - y_a}{x_b - x_a}$.

Remarque 3.12. Ici, les opérations que l'on utilise ne correspondent pas à celle des nombres ordinaires que nous avons l'habitude d'utiliser, mais bien des opérations dans $\mathbb{F}_p$.

On s'intéresse maintenant aux droites du plan affine.
Tout d'abord, pour tout point X $\in \{A, B\}$ sur l'axe des abscisses, il existe une unique droite verticale passant par X. Il y a donc 2 droites verticales, chacune étant composée de 2 points. Il s'agit de la droite passant par les points A et C et de celle passant par les points B et D représentées dans la figure 7.

Ensuite, on s'intéresse aux droites de pente k du plan affine, avec $k \in \{0, 1\}$. Ces 2 droites de pente k sont caractérisées par leur pente et leur point d'intersection avec l'axe des ordonnées, et possèdent chacune 2 points. On définit ainsi $2 \times 2 = 4$ droites supplémentaires.

On a donc défini 6 droites : deux droites verticales, deux droites de pente 0 et deux droites de pente 1. Celles-ci sont représentées sur la figure ci-dessous.

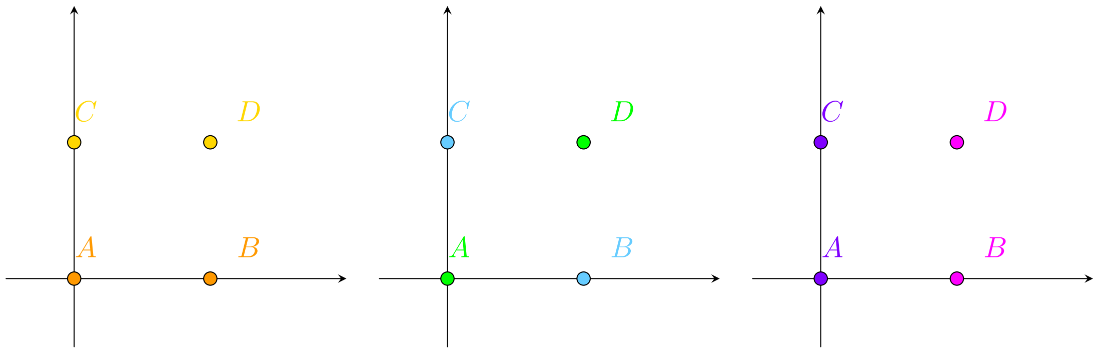

FIGURE 7 – Représentation des droites de pente 0 (à gauche), de pente 1 (au centre) et verticale (à droite)

Pour obtenir les points du plan $P_2(\mathbb{F}_2)$, on complète les points A, B, C, D de $\mathbb{F}_2 \times \mathbb{F}_2$ par des points *à l'infini* E, F et G correspondant respectivement aux droites de pente 0, de pente 1 et de pente verticale.

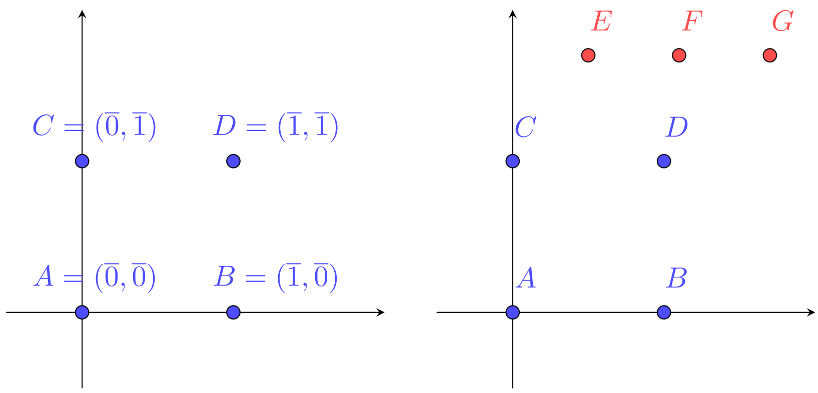

FIGURE 8 – Représentation des points de $\mathbb{F}_2$ (à gauche) et de $P_2(\mathbb{F}_2)$ (à droite)

Pour compléter le plan projectif sur $\mathbb{F}_2$, on ajoute la *droite à l'infini*, composée des points à l'infini E, F et G.

Ainsi les droites du plan $P_2(\mathbb{F}_2)$ sont :

- Les droites de *pente 0*, complétées par le point à l'infini noté E :
  - La droite formée des points A, B et E : d_0.
  - La droite formée des points C, D et E : d_0'.
- Les droites de *pente 1*, complétées par le point à l'infini noté F :
  - La droite formée des points A, D et F : d_1.
  - La droite formée des points B, C et F : d_1'.
- Les droites de *pente verticale*, complétées par le point à l'infini noté G :
  - La droite formée des points A, C et G : d_v.
  - La droite formée des points B, D et G : d_v'.

- La droite *à l'infini* formée des points E, F et G : d_∞.

Le plan de Fano possède donc bien 7 points et 7 droites. En traçant ces points et ces droites, on obtient la représentation du plan de Fano :

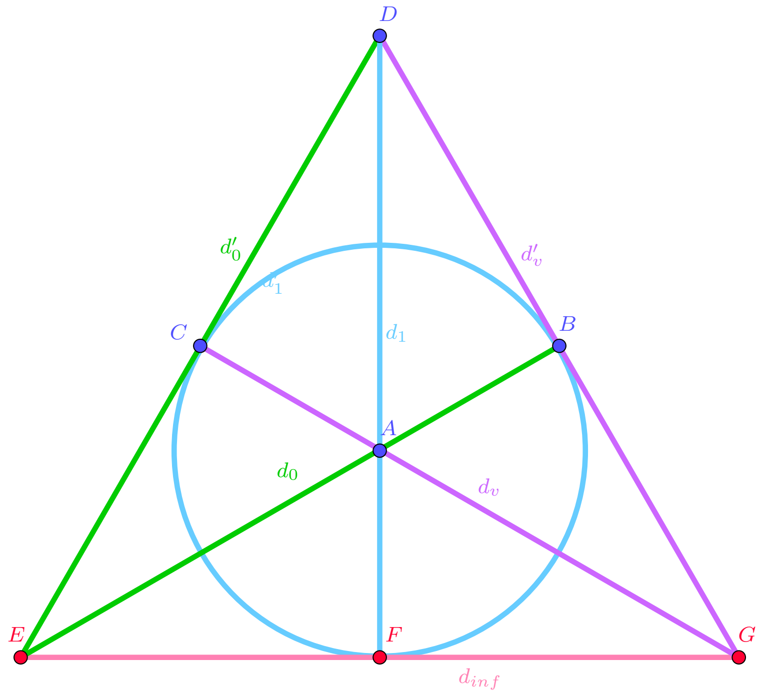

Figure 9 – Représentation du plan de Fano comme plan projectif sur $\mathbb{F}_2$

3.3 Le plan affine sur $\mathbb{F}_7$

À nouveau, on considère d'abord le plan affine sur $\mathbb{F}_7$.
Pour ce faire, on associe à tout couple (x, y) d'éléments de $\mathbb{F}_7 \times \mathbb{F}_7$ un point du plan affine. On obtient la figure suivante :

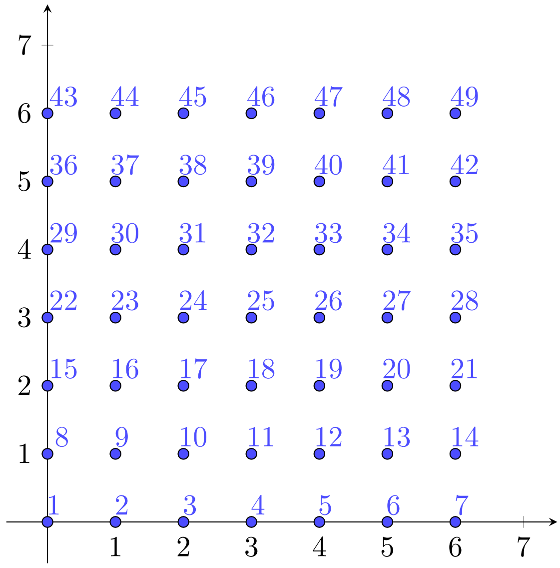

FIGURE 10 – Représentation des 49 points du plan affine sur $\mathbb{F}_7$

On s'intéresse maintenant aux droites du plan affine.
Tout d'abord, pour tout point A $\in \{0, 1, 2, 3, 4, 5, 6\}$ sur l'axe des abscisses, il existe une unique droite verticale passant par A. Il y a donc 7 droites verticales, chacune étant composée de 7 points, que l'on identifie sur la figure ci-dessous.

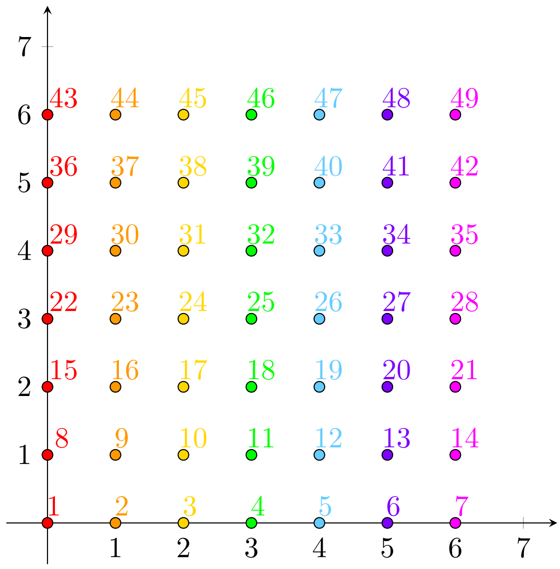

FIGURE 11 – Représentation des 7 droites verticales du plan affine sur $\mathbb{F}_7$

Ensuite, on s'intéresse aux droites de pente k du plan affine, avec $k \in \{0, 1, 2, 3, 4, 5, 6\}$. Ces 7 droites de pente k sont caractérisées par leur pente et leur point d'intersection avec l'axe des ordonnées, et possèdent chacune 7 points. On définit ainsi $7 \times 7 = 49$ droites supplémentaires.

Exemple 3.13. On considère une droite d de pente 2 passant par le point $(1, 0)$.
On note A_i les points de d, avec $i \in \{0, 1, 2, 3, 4, 5, 6\}$. On pose $\mathrm{A}_0 = (0, 1)$.
Comme la pente de la droite d vaut 2, si $A_i = (x, y)$, alors $A_{i+1} = (x +_7 1, y +_7 2)$, où le signe $+_7$ représente l'addition modulo 7.
Ainsi, les points de d sont les points : $A_0 = (0, 1)$; $A_1 = (1, 3)$; $A_2 = (2, 5)$; $A_3 = (3, 0)$; $A_4 = (4, 2)$; $A_5 = (5, 4)$; $A_6 = (6, 6)$.
La droite d correspond à celle représentée en vert à droite de la figure 12 ci-dessous.

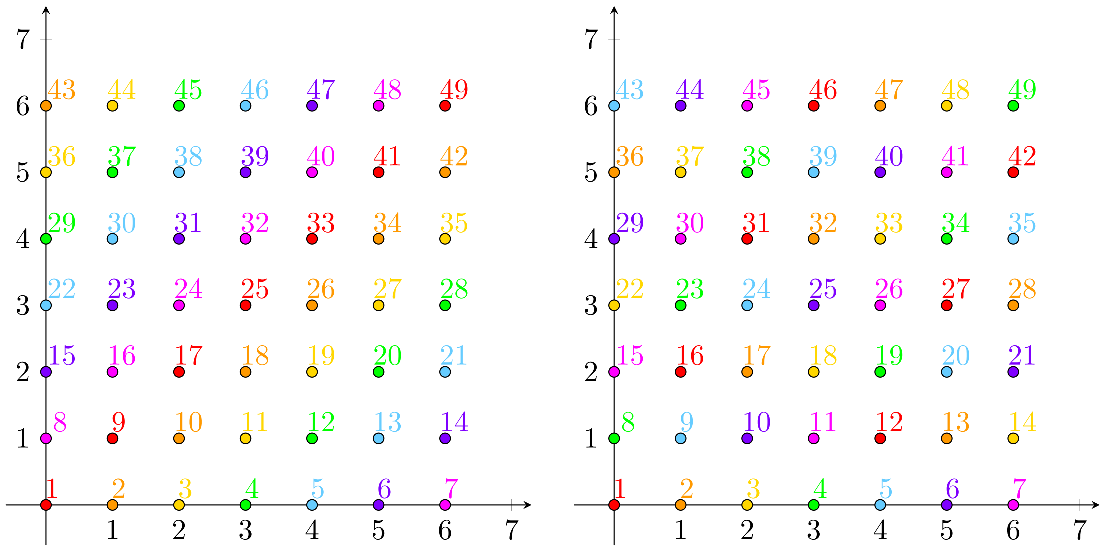

FIGURE 12 – Représentation des droites de pente 1 (à gauche) et de pente 2 (à droite)

Remarque 3.14. Les 56 droites que l'on vient de définir s'intersectent deux à deux en un unique point. Par exemple sur la figure 12, la droite rouge de pente 1 (à gauche) et la droite orange de pente 2 (à droite) s'intersectent en un unique point : celui qui porte le numéro 17.

Construction du plan projectif sur $\mathbb{F}_7$:
Toutes les droites verticales sont parallèles dans le plan affine sur $\mathbb{F}_7$. Elles définissent donc un point *à l'infini* noté $\mathbf{A}_v$ dans le plan projectif associé $P_2(\mathbb{F}_7)$.
De même, les droites de pentes respectives 0, 1, 2, 3, 4, 5 et 6 sont parallèles dans le plan affine sur $\mathbb{F}_7$ et définissent donc un point *à l'infini* dans $P_2(\mathbb{F}_7)$. Ces points sont notés respectivement $\mathbf{A}_0$, $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$, $\mathbf{A}_4$, $\mathbf{A}_5$ et $\mathbf{A}_6$.
Enfin, on complète le plan projectif par la droite *à l'infini* formée de ces points *à l'infini*.

Ainsi le plan projectif $P_2(\mathbb{F}_7)$ possède 57 droites (7 droites verticales, 49 droites de pente k, avec $k \in \{0, 1, 2, 3, 4, 5, 6\}$, et une droite *à l'infini*) et 57 points (les 49 points du plan affine sur $\mathbb{F}_7$ complétés de 8 points *à l'infini*).
La proposition 3.3 est donc bien vérifiée : $P_2(\mathbb{F}_7)$ possède $7^2+7+1 = 57$ points et autant de droites.

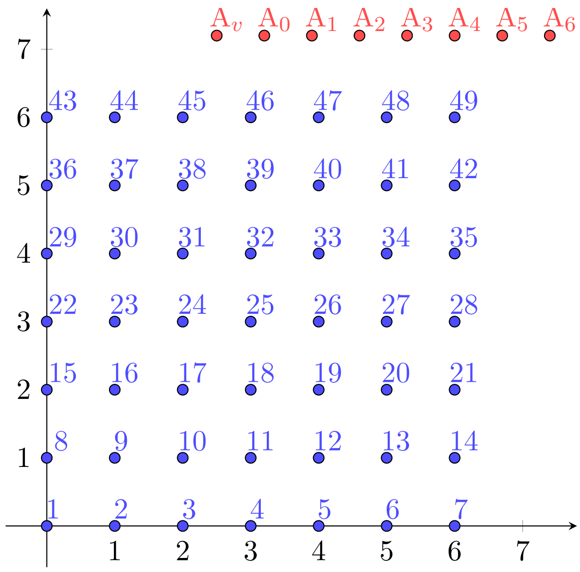

FIGURE 13 – Représentation des 57 points du plan projectif $P_2(\mathbb{F}_7)$

Remarque 3.15. Sur la figure ci-dessus, la position des points rouges est arbitraire car il s'agit des points situés *à l'infini*.

Remarque 3.16. Un plan projectif d'ordre p possède $p^2 + p + 1$ points, et autant de droites.
En effet,

- On sait que chaque droite du plan affine sur $\mathbb{F}_p$ possède p points. Chaque droite projective en contient donc $p + 1$.
  On a également vu que le plan affine sur $\mathbb{F}_p$ possède $p \times p = p^2$ points. On a p pentes possibles pour les droites non verticales, auquel on ajoute la pente infinie pour la droite verticale.
  Il y a donc $p+1$ directions possibles pour les droites. Et on a vu que dans un plan projectif, chaque direction engendre un point à l'infini.
  On obtient donc l'existence de $p + 1$ points à l'infini.
  Le plan projectif $P_2(\mathbb{F}_p)$ contient donc $p^2 + p + 1$ points.
- Tout d'abord, il existe p droites affines verticales. Elles sont les droites d'équation $x = 0, 1, ..., p - 1$.
  Nous allons ensuite essayer de compter les droites affines non verticales. Elles sont caractérisées par leur pente et leur point d'intersection avec l'axe des ordonnées.
  On a p points différents sur l'axe Oy de coordonnées $(0, y)$ avec $y \in \{0, 1, ..., p-1\}$.
  On a vu qu'une droite affine non verticale a p pentes possibles $t \in \{0, 1, ..., p - 1\}$.
  Il y a donc p^2 droites affines non verticales. On ajoute ensuite la droite à l'infini.
  Le plan projectif $P_2(\mathbb{F}_p)$ possède donc $p^2 + p + 1$ droites.

4 Application au jeu de Dobble

4.1 Présentation du jeu

Dobble est constitué de 55 cartes. Sur chaque carte se trouvent 8 symboles différents. Le jeu totalise 57 symboles différents.
Les 57 symboles figurant sur les cartes de Dobble apparaîtront au total 8 fois, sauf 14 d'entre eux qui ne seront présents que 7 fois et un qui n'apparaîtra que 6 fois.
Nous expliquerons cette particularité plus tard.

Par ailleurs, ce jeu possède une propriété remarquable qui va nous rappeler les espaces projectifs : *pour toute paire de cartes, il existe un unique symbole qui figure sur ces deux cartes.*

Exemple 4.1. Prenons par exemple cette paire de cartes :

FIGURE 14 – Paire de cartes Dobble dont l'unique symbole commun est l'araignée

Le but du jeu est très simple : trouver le symbole commun entre deux cartes données le plus rapidement possible.

4.2 Analogie avec les plans projectifs sur $\mathbb{F}_p$

Nous pourrions considérer le plan de Fano comme un mini-jeu de Dobble. En effet, il nous suffirait de considérer les points comme des cartes et les droites comme des symboles.

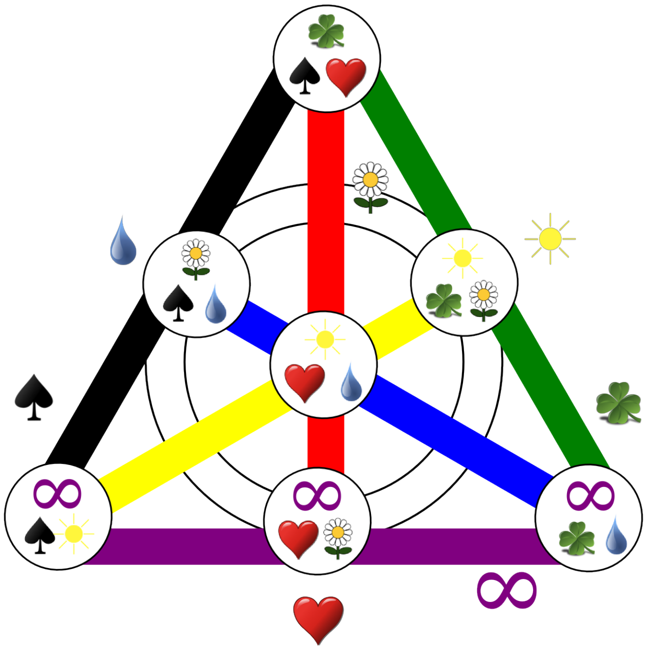

Figure 15 – Représentation d'un jeu de Dobble à 7 cartes

On reconnaît la représentation du plan de Fano, c'est-à-dire le plan projectif sur $\mathbb{F}_2$. Le principe du jeu est bien respecté : chaque carte possède un unique symbole commun avec toute autre carte du jeu. Comme le plan de Fano possède 7 points et 7 droites, le mini-jeu possède 7 cartes et 7 symboles au total. Sur chacune des cartes sont représentés 3 symboles car chaque point du plan de Fano est sur 7 droites.

On peut remarquer l'analogie entre le jeu de Dobble que l'on connaît et le plan projectif sur $\mathbb{F}_7$. Comme précédemment, on peut voir les cartes comme des points et les symboles comme des droites. Ainsi la phrase "la carte contient un symbole" correspond à la phrase "le point est sur la droite". Les 8 symboles sur une même carte correspondent aux 8 droites passant par un même point. De même, les 8 cartes possédant un même symbole correspondent aux 8 points appartenant à une même droite. Chaque symbole de Dobble est donc représenté 8 fois au total.

Comme le plan projectif possède $7^2 + 7 + 1 = 57$ points et 57 droites, le jeu de Dobble devrait contenir 57 cartes et 57 symboles. En réalité, Dobble ne contient que 55 cartes au lieu de 57. Si la raison de ce manque est inconnue, cela ne modifie pas la propriété remarquable selon laquelle chaque carte possède un unique symbole commun avec toute autre carte. Parmi les 57 symboles, 14 d'entre eux ne seront représentés que 7 fois et un symbole (celui commun aux deux cartes manquantes) n'apparaîtra que 6 fois.
On peut également remarquer que si l'on perd des cartes du jeu de Dobble, on peut continuer de jouer sans soucis.

Nous avons démontré que Dobble possède en fait la structure d'un plan projectif d'ordre 7. Nous pourrions de la même façon construire un dobble d'ordre $n > 7$.

Ce nouveau jeu aurait alors $n^2 + n + 1$ cartes, et autant de symboles. En revanche, tous les ordres ne seraient pas possibles (se référer à la partie 3.1).
On pourrait par exemple construire un jeu de Dobble correspondant à un plan projectif d'ordre 11. Il possèderait 133 cartes et autant de symboles.

Références

[1] Maxime Bourrigan. *Dobble et la géométrie finie*. 2011. https://images.math.cnrs.fr/Dobble-et-la-geometrie-finie.html

[2] M. Deléglise. *Plans projectifs, arithmétique modulaire et Dobble*. Université de Lyon, 27 février 2013. http://math.univ-lyon1.fr/deleglis/loisirs.html

[3] Quadriviuum Tremens. *Le Plan Projectif : apprivoiser l'Infini - La Saga des Espaces* #2. https://www.youtube.com/watch?v=kCxEJXINBSo

[4] Sébastien Gandon. *Entre figures et espaces : le cas des diagrammes en géométrie finie*. 2009. http://images.math.cnrs.fr/Entre-figures-et-espaces-le-cas.html

[5] Khalid Koufany. *Généralités sur les anneaux*. Université de Lorraine, 2020.

[6] *The On-Line Encyclopedia of Integer Sequences*. https://oeis.org/A046712

[7] Wikipédia : https://fr.wikipedia.org