

Jeux et plans projectifs

Marc Lorenzi

1er juin 2023

1 Jeux

1.1 Introduction

Dobble® est un jeu comportant 55 cartes circulaires. Sur chacune des cartes figurent 8 symboles. Deux cartes du jeu ont exactement un symbole en commun.



FIGURE 1 – Le jeu Dobble®

À chaque tour de jeu, deux cartes sont piochées dans le paquet. Le joueur qui trouve le premier le symbole commun aux deux cartes gagne le tour.

Derrière ce jeu en apparence très simple se cache une théorie mathématique extrêmement sophistiquée, celle des *plans projectifs finis*.

1.2 Notion de jeu

Définition 1. Un *jeu* est un couple $\mathbb{J} = (S, C)$ où S est un ensemble fini et $C \subseteq \mathcal{P}(S)$, vérifiant les propriétés suivantes.

(J_1) Pour tous $c, c' \in C$ distincts, il existe un unique $s \in S$ tel que $s \in c$ et $s \in c'$.

(J'_1) Il existe un entier $r \geq 2$ tel que pour tout $c \in C$, $|c| = r$.

Pour spécifier le cardinal r des cartes, nous parlerons de r -jeu. Nous noterons cet entier $r(\mathbb{J})$.

Nous appellerons les éléments de S des *symboles* et les éléments de C des *cartes*. Le jeu Dobble[®] est un 8-jeu. Il possède 57 symboles et 55 cartes. D'ici la fin de cette section, nous verrons qu'il devrait normalement y avoir 57 cartes. Les concepteurs du jeu, pour une raison mystérieuse, en ont supprimé deux. Le bruit court que c'était pour des raisons de prix de revient.

Pour tout symbole s et toute carte c , nous noterons

$$C(s) = \{c \in C : s \in c\}$$

$$S(c) = \{s \in S : s \in c\}$$

Pour un r -jeu, on a donc pour tout $c \in C$, $|S(c)| = r$.

Définition 2. Un jeu $\mathbb{J} = (S, C)$ est *symétrique* s'il existe un entier k tel que pour tout $s \in S$,

$$(J'_2) |C(s)| = k$$

Étant donné un jeu symétrique $\mathbb{J}$, nous noterons $k(\mathbb{J}) = |C(s)|$, quantité indépendante du symbole s .

Définition 3. Un jeu $\mathbb{J} = (S, C)$ est *complet* s'il vérifie

(J_2) Pour tous $s, s' \in S$ distincts, il existe un unique $c \in C$ tel que $s \in c$ et $s' \in c$.

Si $\mathbb{J}$ est un jeu complet, nous noterons pour tous s, s' distincts par $c = (ss')$ l'unique carte contenant s et s' .

1.3 Dénombrements

Lemme 1. Soit $\mathbb{J} = (S, C)$ un jeu symétrique. On a

$$r(\mathbb{J})|C| = k(\mathbb{J})|S|$$

Démonstration. Considérons l'ensemble

$$E = \{(s, c) : s \in S, c \in C, s \in c\}$$

Quel est le cardinal de E ? Tout d'abord,

$$E = \bigcup_{s \in S} \{s\} \times C(s)$$

Cette union est disjointe, donc

$$\begin{aligned} |E| &= \sum_{s \in S} |\{s\}| \times |C(s)| \\ &= \sum_{s \in S} |C(s)| \\ &= k(\mathbb{J})|S| \end{aligned}$$

On peut également écrire

$$E = \bigcup_{c \in C} \bigcup_{s \in c} \{(s, c)\}$$

Encore une fois, l'union est disjointe, donc

$$\begin{aligned} |E| &= \sum_{c \in C} \sum_{s \in c} |\{(s, c)\}| \\ &= \sum_{c \in C} \sum_{s \in c} 1 \\ &= \sum_{c \in C} |c| \\ &= r(\mathbb{J})|C| \end{aligned}$$

Ainsi, $|E| = k(\mathbb{J})|S| = r(\mathbb{J})|C|$. $\square$

Lemme 2. Soit $\mathbb{J} = (S, C)$ un jeu symétrique complet. On a

$$(r(\mathbb{J}) - 1)k(\mathbb{J}) = |S| - 1$$

Démonstration. Soit $s \in S$. Considérons l'ensemble

$$E_s = \{(s', (ss')), s' \neq s\}$$

L'application $s' \mapsto (s', (ss'))$ est une bijection de $S \setminus \{s\}$ sur E_s , donc

$$|E_s| = |S| - 1$$

Écrivons

$$E_s = \bigcup_{c \in C(s)} \bigcup_{s' \in S, s' \neq s} \{(s', c)\}$$

Cette union est disjointe, donc

$$\begin{aligned} |E_s| &= \sum_{c \in C(s)} \sum_{s' \in S, s' \neq s} |\{(s', c)\}| \\ &= \sum_{c \in C(s)} |S \setminus \{s\}| \\ &= (r(\mathbb{J}) - 1) \sum_{C \in C(s)} 1 \\ &= (r(\mathbb{J}) - 1) |C(s)| \\ &= (r(\mathbb{J}) - 1) k(\mathbb{J}) \end{aligned}$$

Ainsi, $|E_s| = |S| - 1 = (r(\mathbb{J}) - 1)k(\mathbb{J})$. $\square$

Lemme 3. Soit $\mathbb{J} = (S, C)$ un jeu symétrique complet. On a

$$|C| = k(\mathbb{J}) + (r(\mathbb{J}) - 1)(k(\mathbb{J}) - 1)$$

Démonstration. Pour simplifier les notations, notons $r = r(\mathbb{J})$ et $k = k(\mathbb{J})$. Soit $s_1 \in S$. Soient $c_{1,1}, \dots, c_{1,k}$ les cartes contenant s_1 . Posons

$$c_{1,1} = \{s_1, s_2, \dots, s_r\}$$

Soit $i \in \llbracket 2, r \rrbracket$. L'objet s_i apparaît dans exactement k cartes. Notons ces cartes $c_{i,1}, \dots, c_{i,k}$, où $c_{i,1} = c_{1,1}$. Comme le jeu est complet et que pour tous $i, j \in \llbracket 2, r \rrbracket$ distincts, s_i et s_j appartiennent à $c_{1,1}$, les cartes $c_{i,j}$, $i \in \llbracket 2, r \rrbracket$, $j \in \llbracket 2, k \rrbracket$ sont distinctes, ce qui donne au total $(r - 1)(k - 1)$ cartes. En comptant les cartes $c_{1,1}, \dots, c_{1,k}$, on a donc au moins $k + (r - 1)(k - 1)$ cartes.

Soit c une carte du jeu $\mathbb{J}$. Soit $s' \in C$. Supposons $c \neq c_{1,1}$. Par définition d'un jeu, c et $c_{1,1}$ ont exactement un objet en commun. Il existe donc $i \in \llbracket 1, r \rrbracket$ tel que

$$c \cap c_{1,1} = \{s_i\}$$

De là, puisque $c \neq c_{1,1}$, C est l'une des cartes $c_{i,2}, \dots, c_{i,k}$. Finalement,

$$|C| = \{c_{i,j} : i \in \llbracket 1, r \rrbracket, j \in \llbracket 1, k \rrbracket\}$$

et $|C| = k + (r - 1)(k - 1)$. $\square$

Proposition 4. Soit $\mathbb{J} = (S, C)$ un jeu symétrique complet. On a

$$\begin{aligned} k(\mathbb{J}) &= r(\mathbb{J}) \\ |C| &= r(\mathbb{J})^2 - r(\mathbb{J}) + 1 \\ |S| &= r(\mathbb{J})^2 - r(\mathbb{J}) + 1 \end{aligned}$$

Démonstration. Notons $r = r(\mathbb{J})$ et $k = k(\mathbb{J})$. On a $r|C| = k|S|$. En utilisant les lemmes 2 et 3, on obtient

$$r(k + (r - 1)(k - 1)) = k(k(r - 1) + 1)$$

ou encore

$$rk + r(r - 1)(k - 1) = k^2(r - 1) + k$$

De là,

$$k(r - 1) + r(r - 1)(k - 1) = k^2(r - 1)$$

Comme $r \geq 2$,

$$k + r(k - 1) = k^2$$

qui s'écrit encore

$$k^2 - rk + r - k = 0$$

c'est à dire

$$(k - 1)(k - r) = 0$$

Or, $k \geq 2$, donc $r = k$. Par le lemme 2,

$$|S| = k(r - 1) + 1 = r(r - 1) + 1 = r^2 - r + 1$$

et par le lemme 3,

$$|C| = k + (r - 1)(k - 1) = r + (r - 1)^2 = r^2 - r + 1$$

□

Pour le jeu de Dobble[®], on a $r = 8$. On a donc aussi $k = 8$ et, normalement,

$$|C| = |S| = 8^2 - 8 + 1 = 57$$

Il manque effectivement deux cartes dans la boîte.

1.4 Les petites valeurs de r

Jetons un coup d'oeil aux 2-jeux et aux 3-jeux.

Soit $\mathbb{J} = (S, C)$ un jeu symétrique complet.

Supposons que $\mathbb{J}$ est un 2-jeu. On a $|C| = |S| = 3$ et $r(\mathbb{J}) = k(\mathbb{J}) = 2$. Posons $S = \{A, B, C\}$. On a alors

$$C = \{\{A, B\}, \{A, C\}, \{B, C\}\}$$

Inversement, il est clair que nous avons bien là un 2-jeu symétrique complet. Il existe donc un et un seul 2-jeu, à renommage près des symboles.

Supposons maintenant que $\mathbb{J}$ est un 3-jeu. On a $|C| = |S| = 7$ et $r(\mathbb{J}) = k(\mathbb{J}) = 3$. Posons

$$S = \{A, B, C, D, E, F, G\}$$

Il est un peu moins évident de déterminer C . Supposons que $\{A, B, C\}$ est une carte. Il y a deux autres cartes contenant A , et elles ne contiennent ni B ni C . Il y a trois possibilités pour construire ces deux cartes. Choisissons par exemple $\{A, E, F\}$ et $\{A, D, G\}$.

Passons aux cartes contenant B . Il y a déjà $\{A, B, C\}$. Les deux autres cartes ne peuvent contenir que les symboles D, E, F, G . Comme E et F sont déjà sur une même carte (ainsi que D et E), il y a deux possibilités. Choisissons par exemple $\{B, D, F\}$ et $\{B, E, G\}$.

Nous avons pour l'instant créé les cartes

$$\{A, B, C\}, \{A, E, F\}, \{A, D, G\}, \{B, D, F\}, \{B, E, G\}$$

Créons les cartes contenant C . Il en manque deux, qui ne peuvent contenir, à part C , que les symboles D, E, F, G . Comme D et G appartiennent déjà à une même carte, et également D et F , on doit ajouter la carte $\{C, D, E\}$. Même raisonnement pour ajouter la dernière carte, $\{C, F, G\}$.

Finalement,

$$C = \{\{A, B, C\}, \{A, E, F\}, \{A, D, G\}, \{B, D, F\}, \{B, E, G\}, \{C, D, E\}, \{C, F, G\}\}$$

Inversement, nous avons bien là un 3-jeu symétrique complet. Nous sommes en revanche un peu moins certains de l'unicité d'un tel jeu (il s'avère que c'est bien le cas, mais nous ne le montrerons pas).

Voici une représentation de notre 3-jeu. Les points représentent les symboles et les droites et le cercle sont les cartes.

Nous reviendrons plus loin sur ce diagramme, lorsque nous parlerons du *plan de Fano*.

1.5 Non dégénérescence

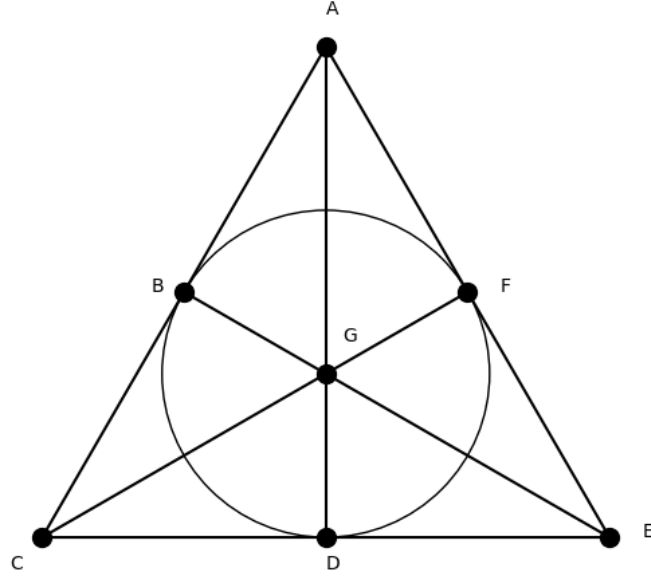


FIGURE 2 – Un 3-jeu complet

Proposition 5. *Soit $r \geq 3$. Soit $\mathbb{J} = (S, C)$ un r -jeu symétrique complet.*

(J_3) Il existe $I \subseteq S$ de cardinal 4 tel que pour tout $c \in C$, c contient au plus deux éléments de I .

Démonstration. On a $|S| = |C| = r^2 - r + 1 = r(r - 1) + 1 \geq 7$.

Soient s_1 et s_2 deux symboles distincts. Soit $c_1 = (s_1 s_2)$. Soit $s_3 \notin c_1$. Soit $c_2 = (s_2 s_3)$. Comme $c_1 \cap c_2$ est un singleton, les cartes c_1 et c_2 contiennent au total $2r - 1$ symboles. Or,

$$|S| - (2r - 1) = r^2 - 3r + 1 = r(r - 3) + 1 \geq 1$$

Il y a donc au un symbole qui n'appartient ni à c_1 ni à c_2 . Appelons-le s_4 . Posons $c_3 = (s_3 s_4)$ et $c_4 = (s_4 s_1)$.

Soi c une carte. Supposons que c contient au moins trois des 4 symboles s_1, s_2, s_3, s_4 . Traitons par exemple le cas où c contient s_1, s_3 et s_4 . Les cartes c et c_3 ont en commun s_3 et s_4 , donc $c = c_3$. De même, $c = c_4$, donc $c_3 = c_4$. De là, comme $s_1 \in c_4$, on a aussi $s_1 \in c_3$. Les symboles s_1, s_2 et s_3 appartiennent ainsi à c_3 . Il en résulte que $(s_1 s_2) = (s_2 s_3)$ et donc $c_1 = c_2$. Contradiction, puisque $s_3 \notin c_1$.

Ainsi, l'ensemble $I = \{s_1, s_2, s_3, s_4\}$ répond à la question. $\square$

Bilan. Retenons les propriétés J_1, J_2, J_3 des jeux symétriques complets, ainsi que les propriétés J'_1 et J'_2 . Nous allons voir dans la prochaine section que J'_1 et J'_2 peuvent se *déduire* de J_1, J_2 et J_3 .

2 Plans projectifs

2.1 Incidence

Donnons-nous deux ensembles P et D . Appelons *points* les éléments de P et *droites* les éléments de D . Donnons nous également une relation $I \subseteq P \times D$. Lorsque $(p, d) \in I$, nous dirons que p est *incident* à d ou que d est *incidente* à p .

Définition 4. Le triplet $\mathbb{P} = (P, D, I)$ est un *plan projectif* lorsque

(P_1) Pour tous points distincts $p, p' \in P$, il existe une unique droite $d \in D$ telle que pId et $p'Id$.

(P_2) Pour toutes droites distinctes $d, d' \in D$, il existe un unique point $p \in P$ tel que pId et pId' .

(P_3) Il existe un ensemble $I \subseteq P$ de quatre points tel que pour toute droite $d \in D$, il existe au plus deux points de I incidents à d .

Tout le monde verra le parallèle entre les axiomes de plan projectif et les axiomes J_1, J_2 et la propriété J_3 des jeux symétriques complets.

Notation. Étant donnés deux points p et p' , nous noterons (pp') l'unique droite incidente à p et p' . Étant données deux droites d et d' , nous noterons $d \cap d'$ l'unique point incident à d et d' . Nous verrons plus loin que le choix du symbole d'intersection est tout à fait pertinent.

Définition 5. Un *quadrangle* est un ensemble de quatre points vérifiant P_3 .

L'axiome P_3 affirme donc l'existence d'un quadrangle. La figure ci-dessous montre, en noir, un quadrangle $\{p_1, p_2, p_3, p_4\}$. La figure montre également les $\binom{4}{2} = 6$ droites incidentes à deux des points du quadrangle. En plus des quatre points du quadrangle, il y a trois points incidents q_1, q_2, q_3 à deux de ces droites. Ils sont représentés en rouge sur la figure.

2.2 Dualité

Considérons la propriété suivante :

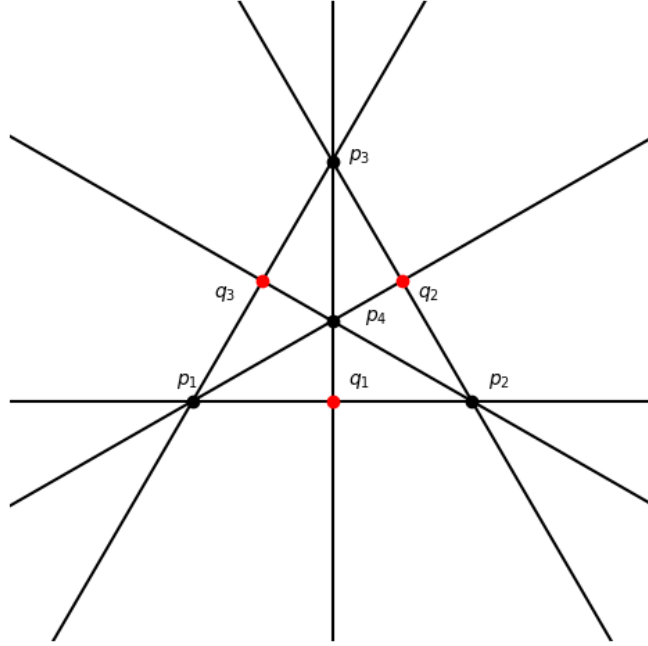


FIGURE 3 – Un quadrangle

(Q₃) Il existe un ensemble $J \subseteq D$ de quatre droites tel que pour tout point $p \in P$, p est incident avec au plus deux des droites de J .

Posons également $Q_1 = P_2$ et $Q_2 = P_1$.

Proposition 6. P_1, P_2 et P_3 impliquent Q_1, Q_2 et Q_3 .

Démonstration. Supposons (P1), (P2) et (P3). Notons $I = \{p_1, p_2, p_3, p_4\}$ un ensemble satisfaisant (P3). Soient $d_1 = (p_1p_2)$, $d_2 = (p_2p_3)$, $d_3 = (p_3p_4)$ et $d_4 = (p_4p_1)$. Soit $J = \{d_1, d_2, d_3, d_4\}$.

Soit $p \in P \setminus I$. Supposons p incident avec au moins trois de ces droites, par exemple d_1, d_2 et d_3 . Les droites d_1 et d_2 sont incidentes avec p et p_2 donc, par l'axiome (P2), $d_1 = d_2$. La droite d_1 est alors incidente avec p_1, p_2 et p_3 ce qui contredit (P3). Ainsi tout point $p \notin I$ est incident avec au plus deux des droites de J .

Soit maintenant $p \in I$. Par exemple, $p = p_1$. Le point p_1 n'est pas incident à d_2 , sinon d_2 serait incidente à p_1, p_2 et p_3 . De même, p_1 n'est pas incident à d_3 . Ainsi on a (Q3). $\square$

Proposition 7. (Q1), (Q2) et (Q3) impliquent (P1), (P2) et (P3).

Démonstration. La preuve est analogue à celle de la proposition précédente, il suffit d'échanger les mots « point » et « droite ». Supposons (P1), (P2) et (Q3). Notons $J = \{d_1, d_2, d_3, d_4\}$ un ensemble satisfaisant (Q3). Soient $p_1 = d_1 \cap d_2$, $p_2 = d_2 \cap d_3$, $p_3 = d_3 \cap d_4$ et $p_4 = d_4 \cap d_1$. Soit $I = \{p_1, p_2, p_3, p_4\}$.

Soit $d \in D \setminus J$. Supposons d incidente avec au moins trois de ces points, par exemple p_1 , p_2 et p_3 . Les points p_1 et p_2 sont incidents avec d et d_2 donc, par l'axiome (P1), $p_1 = p_2$. Le point p_1 est alors incident avec d_1 , d_2 et d_3 ce qui contredit (Q3). Ainsi toute droite $d \notin J$ est incidente avec au plus deux des points de I .

Soit maintenant $d \in J$. Par exemple, $d = d_1$. La droite d_1 n'est pas incidente avec p_2 , sinon p_2 serait incident avec d_1 , d_2 et d_3 . De même, d_1 n'est pas incidente avec p_3 . Ainsi on a (P3). $\square$

Définition 6. Un *quadrilatère* est un ensemble de quatre droites vérifiant (Q3).

Les deux propositions précédentes montrent ainsi que si on a (P1) et (P2), alors l'existence d'un quadrangle équivaut à l'existence d'un quadrilatère.

Définition 7. Soit $\mathbb{P} = (P, D, I)$ un plan projectif. Le *plan dual* de $\mathbb{P}$ est $\mathbb{P}^D = (D, P, I^*)$ où $dI^*p \iff pId$.

Proposition 8. Le dual d'un plan projectif est un plan projectif.

Démonstration. $\mathbb{P}$ vérifie (P1), (P2) et (P3). On a donc (Q1), (Q2) et (Q3). Ces trois propriétés expriment que $\mathbb{P}^D$ est un plan projectif. $\square$

Définition 8. Soit $\mathcal{P}$ une *propriété projective*, c'est à dire une propriété s'exprimant à l'aide des concepts de point, de droite et d'incidence. La *propriété duale* de $\mathcal{P}$ est la propriété $\mathcal{P}^D$ obtenue en remplaçant dans $\mathcal{P}$ chaque occurrence de « point » par « droite » et vice versa.

Nous avons alors le résultat suivant.

Proposition 9. Soit $\mathbb{P}$ un plan projectif. Soit $\mathcal{P}$ une propriété projective vérifiée par $\mathbb{P}$. Alors, $\mathcal{P}^D$ est vérifiée par $\mathbb{P}^D$.

Nous pouvons maintenant énoncer le *principe de dualité*.

Proposition 10. [PRINCIPE DE DUALITÉ]

Soit $\mathcal{P}$ une propriété projective vérifiée par tous les plans projectifs. Alors, $\mathcal{P}^D$ est vérifiée par tous les plans projectifs.

Démonstration. Soit $\mathbb{P}$ un plan projectif. La propriété $\mathcal{P}$ est vérifiée par le plan projectif $\mathbb{P}^D$, donc la propriété $\mathcal{P}^D$ est vérifiée par $\mathbb{P}^{DD} = \mathbb{P}$. $\square$

2.3 Dénombrements

Proposition 11. Soit $\mathbb{P} = (P, D, I)$ un plan projectif. On a $|P| \geq 7$ et $|D| \geq 7$.

Démonstration. La figure 3 résume les étapes du raisonnement que nous allons faire ici. Soit $Q = \{p_1, p_2, p_3, p_4\}$ un quadrangle. Les droites (p_1p_2) et (p_3p_4) sont incidentes à un point $q_1 \notin Q$. De même, (p_1p_3) et (p_2p_4) sont incidentes à un point $q_2 \notin Q$ et (p_1p_4) et (p_2p_3) sont incidentes avec un point $q_3 \notin Q$. Supposons un instant que $q_1 = q_2$. La droite (p_1p_2) est incidente à p_1 , à p_2 , mais aussi à q_1 . De même, la droite (p_2p_4) est incidente à p_2 , à p_4 , mais aussi à $q_2 = q_1$. Les deux droites (p_1p_2) et (p_2p_4) sont ainsi incidentes à q_1 et p_2 . Comme $q_1 \neq p_2$, par l'axiome (P1) ces deux droites sont égales. Les points p_1 , p_2 et p_4 sont donc incidents à une même droite, ce qui contredit (P3). Ainsi, $q_1 \neq q_2$. De même, $q_2 \neq q_3$ et $q_3 \neq q_1$. L'ensemble P contient donc les 7 points distincts $p_1, \dots, p_4, q_1, q_2, q_3$.

Par le principe de dualité, on a aussi $|D| \geq 7$. $\square$

Pour toute droite d , soit $P(d)$ l'ensemble des points incidents avec d :

$$P(d) = \{p \in P : pId\}$$

De même, pour tout point p , soit $D(p)$ l'ensemble des droites incidentes avec p :

$$D(p) = \{d \in D : pId\}$$

Proposition 12. Soit $\mathbb{P} = (P, D, I)$ un plan projectif.

- Pour toute droite d , $|P(d)| \geq 3$.
- Pour tout point p , $|D(p)| \geq 3$.

Démonstration. Soit $I = \{p_1, p_2, p_3, p_4\}$ un quadrangle. Soit d une droite. Par exemple, $p_1, p_2 \notin d$. Soient $d_1 = (p_2p_3)$, $d_2 = (p_1p_3)$ et $d_3 = (p_1p_2)$. Pour $i \in \llbracket 1, 3 \rrbracket$, soit $q_i = d \cap d_i$. Par une preuve analogue à celle de la proposition précédente, les q_i sont trois points distincts incidents avec d . Ainsi, $|P(d)| \geq 3$.

Par dualité, pour tout point p , $|D(p)| \geq 3$. $\square$

Proposition 13. Soit $\mathbb{P} = (P, D, I)$ un plan projectif. Soit p un point. Il existe une droite d telle que p n'est pas incident à d .

Démonstration. Soit $d \in D(p)$. Soit $p' \in P(d)$ distinct de p . Soit $d' \in D(p')$ distincte de d . Par l'axiome P_1 , p n'est pas incident à d' . $\square$

Proposition 14. Soit $\mathbb{P} = (P, D, I)$ un plan projectif fini. Il existe un entier $n \geq 2$ tel que

- Pour toute droite d , $|P(d)| = n + 1$.
- Pour tout point p , $|D(p)| = n + 1$.

Démonstration. Soient d et d' deux droites distinctes. Soit $p = d \cap d'$. Soit $d'' \in D(p)$ distincte de d et d' . Soit $p' \in P(d'')$ distinct de p . Posons

$$P(d) = \{q, q_1, \dots, q_n\}$$

où $n \geq 2$, puisque $|P(d)| \geq 3$. Pour $i \in \llbracket 1, n \rrbracket$, soit $d_i = (p'q_i)$. Soit ensuite $q'_i = d' \cap d_i$. On a donc $p, q'_1, \dots, q'_n \in P(d')$. De là,

$$|P(d')| \geq n + 1 = |P(d)|$$

En échangeant les rôles de d et d' , on obtient l'inégalité inverse. Finalement,

$$|P(d)| = n + 1 = |P(d')|$$

Soit $p \in P$. Soit d une droite telle que $p \notin P(d)$. Posons

$$P(d) = \{p_1, \dots, p_{n+1}\}$$

Pour $i \in \llbracket 1, n + 1 \rrbracket$, soit $d_i = (pp_i)$. Les droites d_i sont distinctes, donc

$$|D(p)| \geq n + 1$$

et

$$D(p) \supseteq \{d_1, \dots, d_{n+1}\}$$

Soit maintenant $d' \in D(p)$. Soit $p' = d \cap d'$. On a alors $p' \in P(d)$ donc p' est l'un des points p_i . De là, d est l'une des droites d_i , et donc

$$D(p) \subseteq \{d_1, \dots, d_{n+1}\}$$

Finalement,

$$D(p) = \{d_1, \dots, d_{n+1}\}$$

et donc $|D(p)| = n + 1$. $\square$

Définition 9. Soit $\mathbb{P}$ un plan projectif fini. L'ordre de $\mathbb{P}$ est l'(unique) entier $n \geq 2$ dont l'existence est prouvée par la proposition 14.

Remarque. L'unicité est évidente. Un plan projectif $\mathbb{P}$ possède au moins un point p (et même 7), et l'ordre de $\mathbb{P}$ est $|D(p)| - 1$.

Proposition 15. Soit $\mathbb{P} = (P, D, I)$ un plan projectif fini. Soit $n \geq 2$ tel que $n + 1$ soit le cardinal commun des ensembles $P(d)$, $d \in D$ et $D(p)$, $p \in P$. On a

$$|P| = |D| = n^2 + n + 1$$

Démonstration. Soit $p \in P$. Tout point de P est incident à une droite incidente à p . On a donc

$$P = \{p\} \cup \bigcup_{d \in D(p)} (P(d) \setminus \{p\})$$

Remarquons que si $d, d' \in D(p)$ sont deux droites distinctes, elles sont par l'axiome P_2 incidentes à un unique point qui est p . L'union ci-dessus est donc une union disjointe. De là,

$$\begin{aligned} |P| &= 1 + \sum_{d \in D(p)} |P(d) \setminus \{p\}| \\ &= 1 + n \sum_{d \in D(p)} 1 \\ &= 1 + n|D(p)| \\ &= n^2 + n + 1 \end{aligned}$$

Par dualité, on a aussi $|D| = n^2 + n + 1$. $\square$

2.4 Isomorphismes

Définition 10. Soient $\mathbb{P} = (P, D, I)$ et $\mathbb{P}' = (P', D', I')$ deux plans projectifs. Un *isomorphisme* de $\mathbb{P}$ sur $\mathbb{P}'$ est un couple (f, g) où $f : P \rightarrow P'$ et $g : D \rightarrow D'$ sont des bijections, vérifiant de plus :

Pour tout point $p \in P$ et toute droite $d \in D$,

$$pId \implies f(p)I'g(d)$$

Deux plans sont isomorphes s'il existe un isomorphisme de l'un sur l'autre.

2.5 Les droites comme ensembles de points

La vision commune que l'on a de la géométrie est qu'une droite *est* un ensemble de points. Nos axiomes de plan projectif n'affirment rien de tel. Nous avons une relation entre les points et les droites (l'incidence) mais les droites ne sont pas des ensembles. Il est cependant possible de montrer que tout

plan projectif est isomorphe à un plan projectif dans lequel les droites *sont* des ensembles de points. C'est ce que nous allons maintenant voir.

Proposition 16. Soit $\mathbb{P} = (P, D, I)$ un plan projectif

- Pour toutes droites d et d' , si $P(d) = P(d')$ alors $d = d'$.
- Pour tous points p et p' , si $D(p) = D(p')$ alors $p = p'$.

Démonstration. $P(d) = P(d')$ contient au moins deux points p et q (et même trois). Par l'axiome P_1 , il existe une unique droite incidente à p et q . Or, d et d' sont incidentes à p et q , donc $d = d'$.

Par dualité, on a aussi le second point. $\square$

Considérons un plan projectif $\mathbb{P} = (P, D, I)$. Considérons $\mathbb{P}' = (P, D', \in)$ où $D' = \{P(d) : d \in D\}$.

Proposition 17. $\mathbb{P}'$ est un plan projectif isomorphe à $\mathbb{P}$.

Démonstration. Soit $f = id_P$. Soit $g : D \rightarrow D'$ définie par $g(d) = P(d)$. La fonction f est évidemment une bijection de P sur P . Par la proposition précédente, g est injective. Par définition même de D' , g est surjective. Ainsi, g est une bijection de D sur D' .

Soient $p \in P$ et $d \in D$. Supposons pId . On a donc $p \in P(d)$, c'est à dire $p \in g(d)$. Ainsi, (f, g) est un isomorphisme du plan projectif $\mathbb{P}$ sur le plan projectif $\mathbb{P}'$. $\square$

2.6 Un exemple minimal - le plan de Fano

Nous avons vu que si $\mathbb{P} = (P, D, I)$ est un plan projectif fini, alors

- $|P| = |D| \geq 7$.
- Pour tout point $p \in P$, $|D(p)| \geq 3$.
- Pour toute droite $d \in D$, $|P(d)| \geq 3$.

Nous allons construire un plan projectif fini $\mathbb{P} = (P, D, I)$. pour lequel ces inégalités sont des égalités.

Posons $P = \llbracket 1, 7 \rrbracket$. Nous écrirons dans la suite les éléments de P par leur représentation en base 2. On a donc

$$P = \{001, 010, 011, 100, 101, 110, 111\}$$

On définit de façon naturelle une addition sur l'ensemble P en posant

$$abc + a'b'c' = (a + a')(b + b')(c + c')$$

où les additions de chiffres se font modulo 2. Remarquons que l'addition ci-dessus est une opération $P \times P \longrightarrow P \cup \{000\}$. Plus précisément, pour tous $x, y \in P$, $x + y = 000$ si et seulement si $x = y$. Remarquons également que pour tous $x, y, z \in P$,

$$x + y = z \iff x + z = y \iff y + z = x$$

Posons $D = P$. Définissons maintenant un « produit scalaire » sur $P \times D$ en posant

$$\langle abc, xyz \rangle = ax + by + cz$$

Définissons une relation d'incidence sur $P \times D$ par

$$pId \iff \langle p, d \rangle = 0$$

Le tableau ci-dessous représente la relation d'incidence. Pour $p \in P$ et $d \in D$, on a pId lorsqu'il y a un 1 dans la case ligne p , colonne d . Remarquons que le tableau est symétrique par rapport à la diagonale, on pourrait donc tout aussi bien prendre le contraire.

	001	010	011	100	101	110	111
001	0	1	0	1	0	1	0
010	1	0	0	1	1	0	0
011	0	0	1	1	0	0	1
100	1	1	1	0	0	0	0
101	0	1	0	0	1	0	1
110	1	0	0	0	0	1	1
111	0	0	1	0	1	1	0

FIGURE 4 – La relation d'incidence dans le plan de Fano

Le schéma ci-dessous représente les points de P et les droites de D .

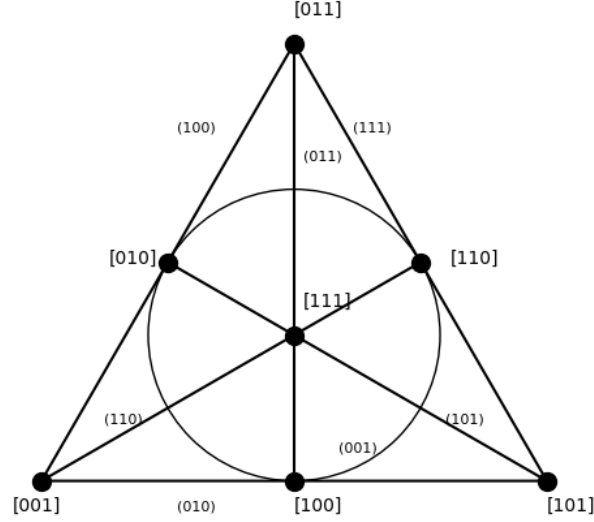


FIGURE 5 – Le plan de Fano

Proposition 18. $\mathbb{P}$ est un plan projectif d'ordre 2.

Démonstration. La table de la relation d'incidence ou le schéma suffisent à se persuader que les axiomes P_1 et P_2 sont vérifiés. Pour l'axiome P_3 , on peut, par exemple, prendre l'ensemble

$$Q = \{001, 101, 011, 111\}$$

qui est bien un quadrangle. $\square$

Nous allons maintenant montrer l'unicité du plan de Fano.

Proposition 19. Il existe, à isomorphisme près, un unique plan projectif fini d'ordre 2.

Démonstration. Soit $\mathbb{P} = (P, D, I)$ un plan projectif fini d'ordre 2. Soit $Q = \{p_1, p_2, p_3, p_4\}$ un quadrangle de $\mathbb{P}$. Reprenons la figure déjà vue plus haut.

Comme $\mathbb{P}$ est d'ordre 2, P est de cardinal 7. Nous avons donc représenté tous les points. Passons aux droites.

La figure comporte 6 droites. Il faut rajouter à celles-ci les droites (q_1q_2) , (q_2q_3) et (q_3q_1) , distinctes des 6 droites déjà présentes. Comme $\mathbb{P}$ est d'ordre 2, il existe exactement 7 droites. Il en résulte que ces trois droites sont égales. Les points q_1 , q_2 et q_3 sont ainsi incidents à une septième (et dernière) droite.

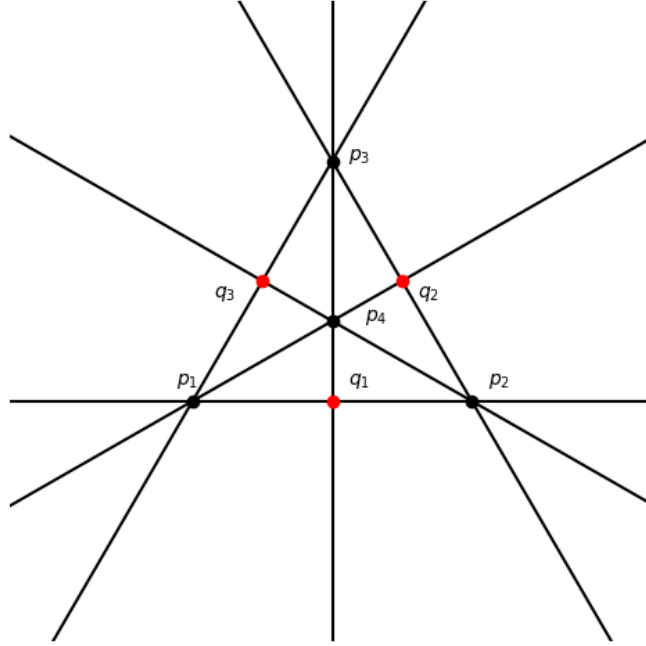


FIGURE 6 – Un quadrangle

En comparant la figure ci-dessus avec celle du plan de Fano, il est maintenant facile de créer un isomorphisme entre ces deux plans projectifs. $\square$

2.7 Retour à Dobble®

Considérons un jeu symétrique complet $\mathbb{J} = (S, C)$, où $r(\mathbb{J}) \geq 3$. Considérons la relation $I \subseteq S \times C$ définie par $sIc \iff s \in c$. Les axiomes J_1 , J_2 et le théorème J_3 montrent que $\mathbb{P} = (S, C, I)$ est un plan projectif fini. En effet, ces deux axiomes et le théorème ne sont autres que les axiomes P_1 , P_2 et P_3 .

Inversement, soit $\mathbb{P} = (P, D, I)$ un plan projectif fini. Posons $D' = \{D(p) : p \in P\}$. Alors, $\mathbb{J} = (P, \tilde{D})$ est un jeu symétrique complet. En effet, J_1 et J_2 ne sont autres que P_1 et P_2 . De plus, on a, par la proposition 14, J'_1 et J'_2 .

Clairement, l'application $\varphi : \mathbb{J} = (S, C) \mapsto \mathbb{P} = (P, D, \in)$ est une bijection de la classe des jeux symétriques complets sur la classe des plans projectifs. Sa réciproque est la fonction $\psi : \mathbb{P} = (P, D, I) \mapsto \mathbb{J} = (P, \tilde{D})$.

Enfin, remarquons que si $\mathbb{J}$ est un n -jeu, où $n \geq 3$, alors $\varphi(\mathbb{J})$ est un plan projectif d'ordre $n - 1$. Le jeu de Dobble, qui est un 8-jeu, est donc associé à un plan projectif d'ordre 7.

3 Une famille de plans projectifs

Nous allons dans cette section construire une famille de plans projectifs particuliers, les *plans arguésiens*.

3.1 Corps finis

Les plans projectifs dont nous allons parler sont construits à partir de *corps finis*. Nous allons brièvement énoncer ce que l'on sait sur les corps finis. Tout d'abord, quel est le cardinal d'un tel corps ?

Proposition 20. *Soit $\mathbb{K}$ un corps fini. Il existe un entier premier p et un entier naturel $n \geq 1$ tels que $|\mathbb{K}| = p^n$.*

Démonstration. Considérons l'application $f : \mathbb{Z} \longrightarrow \mathbb{K}$ définie pour tout $n \in \mathbb{Z}$ par $f(n) = n1_{\mathbb{K}}$. L'application f est un morphisme d'anneaux. Comme $\mathbb{Z}$ est infini et $\mathbb{K}$ est fini, f n'est pas injective, donc son noyau est différent de $\{0\}$. Le noyau d'un morphisme d'anneaux est un idéal de l'anneau de départ. Or, les idéaux de $\mathbb{Z}$ sont les ensembles $p\mathbb{Z}$ où $p \in \mathbb{N}$. Il existe donc $p \geq 1$ tel que

$$\ker f = p\mathbb{Z}$$

Comme $11_{\mathbb{K}} = 1_{\mathbb{K}} \neq 0$, on a $p \geq 2$. Supposons que p ne soit pas un entier premier. Il existe $a, b \in \llbracket 2, p-1 \rrbracket$ tels que $p = ab$. On a alors

$$0 = p1_{\mathbb{K}} = a1_{\mathbb{K}}b1_{\mathbb{K}}$$

Comme $\mathbb{K}$ est un corps, c'est aussi un anneau intègre. On en déduit $a1_{\mathbb{K}} = 0$ ou $b1_{\mathbb{K}} = 0$ et donc $a \in \ker f$ ou $b \in \ker f$. Contradiction, car p est le plus petit élément strictement positif de $\ker f$.

Soient $a, b \in \mathbb{Z}$ tels que $a \equiv b \pmod{p}$. Soit $x \in \mathbb{K}$. On a $a - b \in p\mathbb{Z} = \ker f$, donc

$$(a - b)x = (a - b)1_{\mathbb{K}}x = 0$$

De là, on peut munir le corps $\mathbb{K}$ d'une structure d'espace vectoriel sur le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. L'addition est l'addition usuelle dans $\mathbb{K}$. Puis, pour tout $x \in \mathbb{K}$ et tout $a \in \mathbb{Z}$, on pose $\bar{a}x = ax$, où $\bar{a}$ désigne la classe de a modulo p . $\mathbb{K}$ étant un ensemble fini, c'est nécessairement un espace vectoriel de dimension finie sur le corps $\mathbb{F}$. En appelant n la dimension de $\mathbb{K}$, on a l'isomorphisme d'espaces vectoriels $\mathbb{K} \simeq \mathbb{F}^n$. De là,

$$|\mathbb{K}| = |\mathbb{F}^n| = |\mathbb{F}|^n = p^n$$

□

Se pose maintenant la question de l'existence et de l'unicité. Nous avons à ce sujet un résultat très précis.

Proposition 21. *Soit p un entier premier. Soit $n \geq 1$ un entier naturel. Il existe un corps fini de cardinal p^n . De plus, un tel corps est unique à isomorphisme près.*

Démonstration. La démonstration de ce résultat n'est pas simple, elle utilise des résultats de la théorie des corps. Nous l'admettrons ici. $\square$

3.2 Points

Dans la suite, $\mathbb{K}$ désigne un corps fini de cardinal q . L'ensemble $E = \mathbb{K}^3$ est muni de sa structure naturelle de $\mathbb{K}$ -espace vectoriel de dimension 3. On pose $E' = E \setminus \{0\}$. Définissons une relation $\sim$ sur E' en posant pour tous $u, v \in E'$,

$$u \sim v \iff \exists \lambda \in \mathbb{K}^*, v = \lambda u$$

Dit autrement, $u \sim v$ si et seulement si u et v sont liés.

Proposition 22. *$\sim$ est une relation d'équivalence.*

Démonstration.

- Soit $u \in E'$. On a $u = 1u$, donc $u \sim u$.
- Soient $u, v \in E'$. Supposons $u \sim v$. Soit $\lambda \in \mathbb{K}^*$ tel que $v = \lambda u$. On a alors $u = \frac{1}{\lambda}v$, donc $v \sim u$.
- Soient $u, v, w \in E'$. Supposons $u \sim v$ et $v \sim w$. Soient $\lambda, \mu \in \mathbb{K}^*$ tel que $v = \lambda u$ et $w = \mu v$. On a alors $w = (\lambda\mu)u$, donc $u \sim w$.

$\square$

Nous noterons $P = E' / \sim$. Les éléments de P sont les futurs points de notre plan projectif. Appelons-les tout de suite des *points*.

Si $u = (x, y, z) \in E'$, nous noterons $[u] = [x, y, z] \in P$ la classe de u . Remarquons que $[x, y, z] = [x', y', z']$ si et seulement si il existe $\lambda \in \mathbb{K}^*$ tel que $x' = \lambda x$, $y' = \lambda y$ et $z' = \lambda z$.

Proposition 23. $|P| = q^2 + q + 1$.

Démonstration. Les points de P sont les classes modulo $\sim$. Ils forment donc une partition de E' . Écrivons

$$E' = \bigcup_{p \in P} p$$

Les classes étant disjointes,

$$|E'| = \sum_{p \in P} |p|$$

Soit p un point. Soit $(x, y, z) \in p$. On a

$$p = [x, y, z] = \{\lambda(x, y, z) : \lambda \in \mathbb{K}^*\}$$

Ainsi, $|p| = |\mathbb{K}| - 1 = q - 1$. De là,

$$|E'| = q^3 - 1 = \sum_{p \in P} (q - 1) = (q - 1)|P|$$

Comme $q^3 - 1 = (q - 1)(q^2 + q + 1)$ et $q \neq 1$, on en déduit le résultat. $\square$

3.3 Droites

Définition 11. Soit d un ensemble de points. L'ensemble d est une *droite* s'il existe $(a, b, c) \in E'$ tel que pour tout $[x, y, z] \in P$,

$$ax + by + cz = 0$$

Remarque. La définition ci-dessus a bien un sens, elle ne dépend que de la classe du triplet (x, y, z) modulo $\sim$, et pas de x, y, z .

Nous noterons D l'ensemble des droites. À quelle condition deux équations définissent-elles une même droite ?

Proposition 24. Soient d et d' deux droites d'équations

$$(d) \quad ax + by + cz = 0$$

$$(d') \quad a'x + b'y + c'z = 0$$

On a $d = d'$ si et seulement si $[a, b, c] = [a', b', c']$.

Démonstration. Supposons $d = d'$. Le système

$$\begin{cases} ax + by + cz = 0 \\ a'x + b'y + c'z = 0 \end{cases}$$

est équivalent à sa première équation. C'est donc un système de rang 1. La matrice du système

$$A = \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix}$$

est donc une matrice de rang 1, ses deux lignes sont liées.

La réciproque est évidente. $\square$

3.4 Plan projectif

Posons $\mathbb{P} = (P, D, \in)$.

Proposition 25. $\mathbb{P}$ est un plan projectif.

Démonstration. Il s'agit de prouver que $\mathbb{P}$ vérifie les axiomes P_1 , P_2 et P_3 .

(P_1) Soient $p = [x, y, z]$ et $p' = [x', y', z']$ deux points distincts. Soit

$$(d) \quad ax + by + cz = 0$$

Les points p et p' sont distincts, donc les vecteurs $u = (x, y, z)$ et $u' = (x', y', z')$ sont libres. Le système homogène d'inconnue $(a, b, c) \in \mathbb{K}^3$

$$\begin{cases} ax + by + cz = 0 \\ ax' + by' + cz' = 0 \end{cases}$$

est donc de rang 2. L'ensemble de ses solutions est donc un sous-espace vectoriel de $\mathbb{K}^3$ de dimension $3 - 2 = 1$. Il existe donc, à constante multiplicative non nulle près, un unique triplet non nul $(a, b, c) \in \mathbb{K}^3$ tel que $ax + by + cz = ax' + by' + cz' = 0$. Dit autrement, il existe une unique droite d telle que $p, p' \in d$.

(P_2) Soient d, d' deux droites distinctes. Il existe $(a, b, c) \in E'$ et $(a', b', c') \in E'$ tels que

$$(d) \quad ax + by + cz = 0$$

$$(d') \quad a'x + b'y + c'z = 0$$

Les droites d et d' sont distinctes, donc $(a, b, c) \not\sim (a', b', c')$. Par le même raisonnement que pour P_1 , $d \cap d'$ est un singleton.

(P_3) Soient $p_1 = [0, 0, 1]$, $p_2 = [0, 1, 1]$, $p_3 = [1, 0, 1]$ et $p_4 = [1, 1, 0]$. Soit $I = \{p_1, p_2, p_3, p_4\}$. Soit d une droite d'équation

$$(d) \quad ax + by + cz = 0$$

où $(a, b, c) \neq (0, 0, 0)$.

- Supposons $p_1, p_2, p_3 \in d$. On en déduit $c = 0$, puis $b = 0$ et enfin $a = 0$, contradiction.
- Supposons $p_1, p_2, p_4 \in d$. Comme dans le premier cas, on a une contradiction.
- Supposons $p_1, p_3, p_4 \in d$. On en déduit $c = 0$, puis $a = 0$ et enfin $b = 0$, contradiction.
- Supposons enfin $p_2, p_3, p_4 \in d$. On en déduit $b + c = 0$ puis $a + c = 0$ et enfin $a + b = 0$. De ces trois égalités, il vient $a = b = c = 0$. Encore une fois, on aboutit à une contradiction.

Ainsi, toute droite d contient au plus deux des points de I . L'axiome P_3 est bien vérifié. $\square$

Proposition 26. $\mathbb{P}$ est un plan projectif d'ordre q , où $q = |\mathbb{K}|$.

Démonstration. Nous avons déjà vu que $|P| = q^2 + q + 1$. Soit r l'ordre de $\mathbb{P}$. On a, par définition de l'ordre d'un plan projectif fini,

$$|P| = r^2 + r + 1$$

Ainsi, $p^2 + p + 1 = r^2 + r + 1$, ou encore

$$p^2 - r^2 + p - r = 0$$

qui se factorise en

$$(p - r)(p + r + 1) = 0$$

Comme $p + r + 1 > 0$, $r = p$. $\square$

Corollaire 27.

- Pour tout point p , $|D(p)| = q$.
- Pour toute droite d , $|P(d)| = q$.

Nous savons donc construire des plans projectifs d'ordre p^n pour tout nombre premier p et tout entier non nul n . Les premiers ordres de ces plans sont

$$2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19$$

Nous voyons que le premier ordre absent de la liste est 6. Nous verrons plus loin qu'il n'existe pas de plan projectif fini d'ordre 6. Il reste à l'heure actuelle une question ouverte.

4 Le théorème de Bruck-Ryser

Le théorème de Bruck-Ryser donne des conditions nécessaires sur l'ordre d'un plan projectif fini. Autrement dit, il permet d'affirmer que pour certains entiers $n \geq 2$, il n'existe pas de plan projectif fini d'ordre n . Avant d'énoncer et de montrer ce théorème, introduisons quelques notions supplémentaires.

4.1 Matrices d'incidence

Soit $\mathbb{P} = (P, D, I)$ un plan projectif fini d'ordre $n \geq 2$. Posons $m = n^2 + n + 1$. Les ensembles P et D sont finis, de cardinal m . La matrice d'incidence de

$\mathbb{P}$ est la matrice $A \in \mathcal{M}_m(\mathbb{F}_2)$ définie pour tout $p \in P$ et tout $d \in D$ par $A_{pd} = 1$ si pId et $A_{pd} = 0$ sinon. Nous notons dans la suite $[pId] = 1$ si pId et $[pId] = 0$ sinon.

Remarque. Nous avons défini A en l'indexant par les points de P et les droites de D . En toute rigueur, il aurait fallu l'indexer par les entiers de $\llbracket 1, m \rrbracket$. Pour cela, il conviendrait d'indexer les points et les droites. Il n'y a alors pas unicité de la matrice A , puisque des permutations de lignes ou de colonnes correspondent à différentes indexations de P et D .

Exemple. Rappelons que le plan de Fano est $\mathbb{P} = (P, D, I)$ où $P = D = \llbracket 1, 7 \rrbracket$. La matrice d'incidence de $\mathbb{P}$ est

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Proposition 28.

$$AA^T = nI_m + J_m$$

où I_m est la matrice identité d'ordre m et $J_m \in \mathcal{M}_m(\mathbb{F}_2)$ est la matrice dont tous les coefficients sont égaux à 1.

Démonstration. Soient $p, q \in P$. On a

$$(AA^T)_{pq} = \sum_{d \in D} A_{pd}A_{qd} = \sum_{d \in D} [pId][qId]$$

Si $p = q$, alors

$$(AA^T)_{pq} = \sum_{k=1}^m [pId]^2 = \sum_{p \in P(d)} 1 = |P(d)| = n + 1$$

Si $p \neq q$, il existe une unique droite d_0 incidente à p et q . On a alors pour toute droite d , $[pId][qId] = \delta_{dd_0}$, donc $(AA^T)_{pq} = 1$. $\square$

Proposition 29.

$$\det A = \pm(n+1)n^{\frac{1}{2}n(n+1)}$$

Remarque. La matrice A est « unique » à permutation près des lignes et des colonnes. Son déterminant n'est donc défini qu'au signe près.

Démonstration. Considérons la matrice $B = AA^T$. Par la proposition précédente,

$$B = \begin{pmatrix} n+1 & 1 & \dots & 1 & 1 \\ 1 & n+1 & \dots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \dots & n+1 & 1 \\ 1 & 1 & \dots & 1 & n+1 \end{pmatrix}$$

En soustrayant la première ligne de $\det B$ à toutes les autres, il vient

$$\det(B) = \begin{vmatrix} n+1 & 1 & \dots & 1 & 1 \\ -n & n & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -n & 0 & \dots & n & 0 \\ -n & 0 & \dots & 0 & n \end{vmatrix}$$

Ajoutons à la première colonne la somme des autres colonnes. Rappelons que B est une matrice de taille $m = n^2 + n + 1$. On a donc

$$n+1 + (m-1) = n+m = (n+1)^2$$

De là,

$$\det(B) = \begin{vmatrix} (n+1)^2 & 1 & \dots & 1 & 1 \\ 0 & n & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & n & 0 \\ 0 & 0 & \dots & 0 & n \end{vmatrix}$$

On a là le déterminant d'une matrice triangulaire supérieure. Ainsi,

$$\det(B) = (n+1)^2 n^{m-1} = (n+1)^2 n^{n(n+1)}$$

Par ailleurs,

$$\det(B) = \det(AA^T) = \det(A) \det(A^T) = \det(A)^2$$

d'où le résultat. $\square$

4.2 Quelques résultats préliminaires

Dans ce paragraphe, nous allons présenter trois résultats d'arithmétique concernant les sommes de carrés. Nous admettrons deux de ces trois résultats. Leur démonstration peut se faire de façon élémentaire mais nous éloignerait de notre sujet, celui des plans projectifs.

Proposition 30. [THÉORÈME DES QUATRE CARRÉS DE LAGRANGE]

Soit $n \in \mathbb{N}$. Il existe $a, b, c, d \in \mathbb{N}$ tels que

$$n = a^2 + b^2 + c^2 + d^2$$

Démonstration. Admise. $\square$

Le second résultat admet une preuve élémentaire. En réalité, la preuve que nous allons donner nous cache le fond du sujet, qui concerne le corps des quaternions.

Proposition 31. Soient $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 \in \mathbb{Z}$. Soit

$$B = \begin{pmatrix} b_1 & b_2 & b_3 & b_4 \\ -b_2 & b_1 & -b_4 & b_3 \\ -b_3 & b_4 & b_1 & -b_2 \\ -b_4 & -b_3 & b_2 & b_1 \end{pmatrix}$$

On a $\det(B) = 0$ si et seulement si $b_1 = b_2 = b_3 = b_4 = 0$. De plus, en posant

$$(c_1 \ c_2 \ c_3 \ c_4) = (a_1 \ a_2 \ a_3 \ a_4) B$$

on a

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = c_1^2 + c_2^2 + c_3^2 + c_4^2$$

Démonstration. Posons $a = (a_1 \ a_2 \ a_3 \ a_4)$, et de même pour b et c . On vérifie facilement que

$$BB^T = (b_1^2 + b_2^2 + b_3^2 + b_4^2)I_4 = bb^T I_4$$

On en déduit que

$$(\det B)^2 = (bb^T)^2$$

On a donc $\det B = 0$ si et seulement si

$$0 = bb^T = b_1^2 + b_2^2 + b_3^2 + b_4^2$$

c'est à dire $b_1 = b_2 = b_3 = b_4 = 0$. Enfin,

$$cc^T = aBB^T a^T = abb^T I_4 a^T = aa^T bb^T$$

d'où l'égalité voulue. $\square$

La dernière propriété dont nous aurons besoin pour la preuve du théorème de Bruck-Ryser se montre de façon élégante en utilisant l'anneau $\mathbb{Z}[i]$ des entiers de Gauss. Nous admettrons sa preuve.

Proposition 32. Soit $n \in \mathbb{N}$. On suppose qu'il existe $a, b \in \mathbb{Q}$ tels que $n = a^2 + b^2$. Alors, il existe $a, b \in \mathbb{N}$ tels que $n = a^2 + b^2$.

Démonstration. Admise. $\square$

4.3 Le théorème de Bruck-Ryser

Nous pouvons maintenant aborder le théorème de Bruck-Ryser. Son énoncé est très simple, sa preuve l'est beaucoup moins.

Proposition 33. [BRUCK-RYSER]

Soit $n \in \mathbb{N}$. On suppose $n \equiv 1 \pmod{4}$ ou $n \equiv 2 \pmod{4}$. S'il existe un plan projectif fini d'ordre n , alors il existe deux d'entiers $a, b \in \mathbb{N}$ tels que $n = a^2 + b^2$.

Démonstration. Soit $\mathbb{P}$ un plan projectif fini d'ordre $n \geq 2$. Notons $m = n^2 + n + 1$. Soit A une matrice d'incidence de $\mathbb{P}$.

Donnons-nous $x_1, \dots, x_{m+1} \in \mathbb{Z}$. Soit $x = (x_1 \ \dots \ x_m)$. Soit

$$z = (z_1 \ \dots \ z_m) = xA$$

Posons également, de façon arbitraire, $z_{m+1} = 0$. On a, par la proposition 28,

$$zz^T = xAA^T x^T = x(nI_m + J_m)x^T = nxx^T + xJ_mx^T$$

Remarquons que

$$xJ_mx^T = \left(\sum_{i=1}^m x_i \right)^2 = t^2$$

et donc

$$zz^T = n \sum_{i=1}^m x_i^2 + t^2$$

En ajoutant nx_{m+1}^2 des deux côtés de l'égalité, on obtient

$$\sum_{i=1}^m z_i^2 + nx_{m+1}^2 = n \sum_{i=1}^{m+1} x_i^2 + t^2$$

Comme $n \equiv 1$ ou 2 modulo 4 , on a $m+1 = n^2 + n + 2 \equiv 0 \pmod{4}$. Ceci permet de regrouper quatre par quatre les termes de la somme du membre de droite de l'égalité. Écrivons donc

$$\sum_{i=1}^m z_i^2 + nx_{m+1}^2 = n \sum_{i=0}^{\frac{m+1}{4}-1} (x_{4i+1}^2 + x_{4i+2}^2 + x_{4i+3}^2 + x_{4i+4}^2) + t^2$$

Par le théorème des quatre carrés de Lagrange, il existe $a, b, c, d \in \mathbb{N}$ tels que $n = a^2 + b^2 + c^2 + d^2$. On a donc

$$\sum_{i=1}^m z_i^2 + nx_{m+1}^2 = \sum_{i=0}^{\frac{m+1}{4}-1} (x_{4i+1}^2 + x_{4i+2}^2 + x_{4i+3}^2 + x_{4i+4}^2)(a^2 + b^2 + c^2 + d^2) + t^2$$

Soit $y = (y_1, \dots, y_{m+1})$ tel que pour tout $i \in \llbracket 0, \frac{m+1}{4} - 1 \rrbracket$,

$$(y_{4i+1} \ y_{4i+2} \ y_{4i+3} \ y_{4i+4}) = (x_{4i+1} \ x_{4i+2} \ x_{4i+3} \ x_{4i+4})B$$

où B est la matrice inversible construite à la proposition 31, avec $b_1 = a$, $b_2 = b$, $b_3 = c$, $b_4 = d$. On a alors

$$\sum_{i=1}^m z_i^2 + nx_{m+1}^2 = \sum_{i=0}^{\frac{m+1}{4}-1} (y_{4i+1}^2 + y_{4i+2}^2 + y_{4i+3}^2 + y_{4i+4}^2) + t^2 = \sum_{i=1}^{m+1} y_i^2 + t^2$$

Choisissons maintenant judicieusement $x_1, \dots, x_m$. Pour tout $i \in \llbracket 0, \frac{m+1}{4} - 1 \rrbracket$, posons

$$(x_{4i+1} \ x_{4i+2} \ x_{4i+3} \ x_{4i+4}) = (z_{4i+1} \ z_{4i+2} \ z_{4i+3} \ z_{4i+4})B^{-1}$$

On a donc maintenant

$$(y_{4i+1} \ y_{4i+2} \ y_{4i+3} \ y_{4i+4}) = (z_{4i+1} \ z_{4i+2} \ z_{4i+3} \ z_{4i+4})$$

Ainsi, pour tout $i \in \llbracket 1, m \rrbracket$, $y_i = z_i$. De

$$\sum_{i=1}^m z_i^2 + nx_{m+1}^2 = \sum_{i=1}^{m+1} y_i^2 + t^2$$

on tire alors

$$nx_{m+1}^2 = y_{m+1}^2 + t^2$$

d'où

$$n = \left(\frac{y_{m+1}}{x_{m+1}} \right)^2 + \left(\frac{t}{x_{m+1}} \right)^2$$

Ainsi, n est la somme des carrés de deux rationnels. Par la proposition 32, n est la somme des carrés de deux entiers. $\square$

4.4 Bilan

Il y a 9 entiers $n \leq 50$ pour lesquels le théorème de Bruck-Ryser exclut l'existence d'un plan projectif d'ordre n . Ces entiers sont

$$6, 14, 21, 22, 30, 33, 38, 42, 46$$

Notre construction des plans arguésiens montre que si n est une puissance d'un nombre premier, il existe un plan arguésien d'ordre n . Les 23 entiers $n \leq 50$ pour lesquels il existe un plan arguésien d'ordre n sont

2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 37, 41, 43, 47, 49

Les 17 entiers qui échappent au recensement sont

10, 12, 15, 18, 20, 24, 26, 28, 34, 35, 36, 39, 40, 44, 45, 48, 50

Que sait-on au sujet de ces entiers ? En réalité très peu de choses.