Corps et plans projectifs finis

KADDOURI Abdelkayoum, 18443

Table des matières

Introduction

Les plans projectifs sont des objets mathématiques qui relèvent de la géométrie algébrique. De manière analogue à la géométrie euclidienne classique, ces objets sont définis par des axiomes fondamentaux qui leurs confèrent une symétrie remarquable. Dans ce document, nous explorerons les propriétés des plans projectifs finis, en adoptant d'abord une approche axiomatique, puis une autre approche constructive fondée sur l'algèbre linéaire et sur les corps finis.

Dans le cadre axiomatique, nous examinerons les fondements des plans projectifs en établissant quelques résultats fondamentaux. Ensuite, nous aborderons la caractérisation des corps finis, objets qui permettent d'exhiber une construction de certains plans projectifs.

1 Les plans projectifs finis

Définition 1. *Un plan projectif $\mathbb{P}$ est la donnée d'un triplet d'ensembles (P, D, I), avec $I \subset P \times D$, où P est l'ensemble des points, D l'ensemble des droites, et I la relation d'incidence,vérifiant :*

- *Axiome 1 : Chaque 2 points distincts sont incidents à exactement une droite :* $\forall (A, B) \in P^2, A \neq B, \exists! d \in D, \{(A, d), (B, d)\} \subset I$
- *Axiome 2 : Chaque 2 droites distinctes sont incidentes à exactement un point :* $\forall (d, d') \in D^2, d \neq d', \exists! A \in P, \{(A, d), (A, d')\} \subset I$
- *Axiome 3 : Il existe (un quadrilatère) 4 points tels qu'aucune droite ne soit incidente à 3 points parmi eux .*

On dit que $\mathbb{P}$ est fini si et seulement si P est fini, ce qui équivaut à D fini.

Notation 1. *Dans la suite, on note les points par $A, B, ...$, les droites par d_i.*

$A \in d$ signifiera $(A, d) \in I$, ou encore A indicent à d. Dans le cas contraire, on note $A \notin d$.

AB désignera la droite incidente à A et B et $l_1 \cap l_2$ l'unique point incident à l_1 et l_2.

Lemme 1.1. *Un plan projectif a au moins quatre droites distinctes telles que chaque trois droites ne s'intersectent pas au même point.*

Démonstration. On prend $S = \{A, B, C, D\}$ donné par Axiome 3, les droites AB, BC, CD et DE conviennent. □

Définition 2. *Soit P une proposition sur (P, D, I) les droites et les points d'un plan projectif, la proposition duale F' de F est la proposition qui porte sur le triplet (P', D', I') avec $P = D'$, $D = P'$ et $I' = \{(d, A) : (A, d) \in I\}$.*
Cela revient à intervertir les droites et les points.

On a ainsi les nouveaux axiomes suivants :

- *Axiome 1' : Chaque 2 droites distinctes sont incidentes exactement à un point :*
  $\forall (d, d') \in D^2, d \neq d', \exists! A \in P, \{(A, d), (A, d')\} \subset I$
- *Axiome 2' : Chaque 2 points distincts sont incidents à exactement une droite :*
  $\forall (A, B) \in P^2, A \neq B, \exists! d \in D, \{(A, d), (B, d)\} \subset I$
- *Axiome 3' : Il existe quatre droites distinctes telles que chaque trois droites ne s'intersectent pas au même point.*

Théorème 1.1. *Les deux ensembles d'axiomes sont équivalents.*

Démonstration. Axiome 1 = Axiome 2' et Axiome 2 = Axiome 1', et par le Lemme 2, le premier ensemble d'axiomes implique le deuxième. Supposons le deuxième ensemble d'axiomes, soient l_1, l_2, l_3, l_4 les droites de l'axiome 3', soient A, B, C, D tels que
$l_1 = AB, l_2 = BC, l_3 = CD, l_4 = DA$, alors on a Axiome 3 avec A, B, C et D. □

Ce qui précède montre la dualité point - droite et permet de faciliter les preuves.

Lemme 1.2. *Soit A et d un point et une droite d'un plan projectif fini, avec A non incident à d, et $n \in \mathbb{N}$. Alors d est incidente à $n+1$ points si et seulement si A est incident à $n+1$ droites.*

Démonstration. Supposons que l a n points, les droites passantes par A et qui rencontrent l sont au nombre des points sur l. Et la réciproque est vraie par dualité. □

Théorème 1.2. *Soit $\mathbb{P} = (P, D, I)$ un plan projectif fini, alors il existe un entier $n \geq 2$ tel que :*

— *Tout point est incident à $n+1$ droites.*
— *Toute droite est incidente à $n+1$ points.*

Démonstration. Soit $ABCD$ le quadrilatère de l'Axiome 3, chaque point est au moins sur 3 droites. Soit n l'entier tel que A soit sur $n+1$ droites. Les droites BC, CD et BD ont chacune $n+1$ points d'après le lemme, et tout autre point du plan n'est pas incident à l'une des 3 droites. D'après le lemme, il est incident à $n+1$ droites.
Le second point s'obtient par un argument de dualité. □

Définition 3. *On définit l'ordre d'un plan projectif fini comme l'entier n du théorème précédent.*

Théorème 1.3. *Si $\mathbb{P} = (P, D, I)$ est un plan projectif d'ordre n, alors $card(P) = card(D) = n^2 + n + 1$.*

Démonstration. Soit A un point, il est incident à $n+1$ droites, chacune a n autres points, déterminés de manière unique, et chaque point différent de A est incident à une droite qui passe par A, il y a donc $n(n+1)+1 = n^2+n+1$ points. Le reste se déduit par dualité. □

2 Les corps finis

Une des manières de construire des plans projectifs finis et d'utiliser des espaces vectoriels sur des corps finis, nous montrons donc la caractérisation suivante de ces derniers :

Théorème 2.1. *Soit $\mathbb{K}$ un corps (commutatif) fini, alors $card(\mathbb{K}) = p^n$ avec p premier et $n \in \mathbb{N}^*$. Réciproquement, pour p premier et $n \in \mathbb{N}^*$, il existe un corps fini de cardinal p^n.*

Démonstration. Si K est un corps fini, sa caractéristique est un nombre premier p, donc K est naturellement muni d'une structure de $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel, il est donc isomorphe à $(\mathbb{F}_p)^n$ pour un entier n, donc il est de cardinal p^n. La réciproque utilise le résultat du théorème en dessous : si Q est un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$, l'anneau $\mathbb{K} = \mathbb{F}_p[X]/(Q)$ est un corps (en écrivant une relation de Bezout), de plus, $\mathbb{K} = \{a_{n-1}X^{n-1} + \cdots + a_0/(a_0, \cdots, a_{n-1}) \in (\mathbb{F}_p)^n\}$, donc $card(\mathbb{K}) = p^n$ □

Dans la démonstration précédente, on a besoin du résultat suivant :

Théorème 2.2. *Pour tout p premier et $n \in \mathbb{N}$, il existe un polynôme irréductible dans $\mathbb{F}_p[X]$ de degré n.*

Démontrons d'abord quelques lemmes.

Notation 2. *On note :*
$U_{p,n}$ *: l'ensemble des polynômes unitaires de degré n dans* $\mathbb{F}_p[X]$
$I_{p,n}$ *: l'ensemble des polynômes irréductibles de degré n dans* $\mathbb{F}_p[X]$
$i_{p,n} = card(I_{p,n})$

Le but est de montrer que $i_{p,n} \neq 0$.

Lemme 2.1. *Si* $Q \in I_{p,d}$*, alors* $Q|X^{p^n} - X$ *si et seulement si* $d|n$.

Démonstration. Supposons $d|n$ et montrons que, dans le corps $\mathbb{K} = \mathbb{F}_p[X]/(Q)$ (qui est de cardinal p^d), on a $\overline{X}^{p^n} - \overline{X} = \overline{0}$, en effet : $\mathbb{K}^*$ est d'ordre $p^d - 1$, donc pour tout x dans K : $x^{p^d} = x$, par récurrence : $x^{p^{dk}} = x$ pour tout $k \in \mathbb{N}$. Donc on a bien $\overline{X}^{p^n} - \overline{X} = \overline{0}$.
Réciproquement, supposons que $\overline{X}^{p^n} = \overline{X}$, si $y \in \mathbb{K}$, $y = R(\overline{X})$ avec $R \in \mathbb{F}_p[X]$. Un calcul dans $\mathbb{F}_p[X]$ permet d'affirmer $R(\overline{X})^{p^n} = R(\overline{X}^{p^n}) = R(\overline{X})$, donc $y^{p^n} = y$.
Écrivons la division euclidienne : $n = qd + r$, alors pour tout $y \in \mathbb{F}_p[X]$, $y^{p^n} = (y^{p^d})^{p^r} = y$ car $card(\mathbb{K}*) = p^d - 1$, donc le polynôme $Y^{p^r} - Y$ admet au moins p^d racines (les éléments de $\mathbb{K}$), ce qui n'est possible que si $r = 0$, ou encore si $d|n$. □

Lemme 2.2. $X^{p^n} - X = \prod_{d|n} \prod_{Q \in I_{p,d}} Q$

Démonstration. ce qui précède assure que $\prod_{d|n} \prod_{Q \in I_{p,d}} Q | X^{p^n} - X$, et les facteurs irréductibles de $X^{p^n} - X$ sont les $Q \in I_{p,d}$ avec $d|n$, de plus, $X^{p^n} - X$ est sans facteur carré car sa dérivée est -1, d'où l'égalité car les deux polynômes sont unitaires. □

On arrive ainsi à démontrer le théorème :

Démonstration. En prenant le degré de l'égalité précédente, on a $p^n = \sum_{d|n} d i_{p,d}$, donc $d i_{p,d} \leq p^d$. Si $i_{p,n} = 0$, $p^n = \sum_{d|n} d i_{p,d} \leq \sum_{k=0}^{n-1} p^k = \frac{p^n - 1}{p-1} < p^n$, ce qui est exclu. ainsi on a l'existence d'un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$ □

3 Les espaces projectifs

On a pu établir la caractérisation des corps finis, cela servira à construire certains plans projectifs finis à l'aide des espaces projectifs.

Définition 4. *Soit* $\mathbb{K}$ *un corps et* E *un* $\mathbb{K}$*-espace vectoriel de dimension* 3 *(typiquement* $\mathbb{K}^3$*), l'espace projectif* $\mathbb{P}_E(\mathbb{K})$ *est le triplet* (P, D, I) *où* P *est l'ensemble des droites de* E*,* D *l'ensemble de ses plans (sous-espaces de dimension* 2*) et tel que* $(A, d) \in I$ *si et seulement si* $A \subset d$ *(donc la droite* A *est dans le plan* d*).*

Vu les notations, il est naturel de penser que les espaces projectifs sont des plans projectifs, ce qui est vrai :

Lemme 3.1. $\mathbb{P}_E(\mathbb{K})$ *est un plan projectif.*

Démonstration. Soient l, l' deux plans vectoriels distincts de E, $dim(l \cap l') = 1$ (sinon, soit $l = l'$, soit les deux sont en somme directe), il existe donc une droite vectorielle A dans l'intersection, unique pour des raisons de dimension.
Si A et B sont deux droites vectorielles distinctes de E, le seul plan contenant A et B est $Vect(A, B)$, et il est unique.
Soit (e_1, e_2, e_3) une famille libre de vecteurs de E, les droites vectorielles E :
$Vect(e1), Vect(e_2), Vect(e_3), Vect(e_1 + e_2 + e_3)$ constituent des points qui vérifient l'Axiome 3 : si un plan contient 3 de ses vecteurs, il contient les 4, ce qui est exclu par indépendance. □

Théorème 3.1. *Pour tout p premier et* $n \in \mathbb{N}$*, il existe un plan projectif fini d'ordre* p^n*.*

Démonstration. Soit $\mathbb{P} = \mathbb{P}_{\mathbb{F}_{p^n}}(\mathbb{F}_{p^n}^3)$, soit d un plan vectoriel de $\mathbb{F}_{p^n}^3$, on peut écrire $d = \{ae_1 + be_2 / a, b \in \mathbb{F}_p\}$, avec (e_1, e_2) libre.
Dénombrer les points de d revient à dénombrer les $ae_1 + be_2$, qui s'écrivent de manière unique $u + cv$ avec $c \in \mathbb{F}_{p^n}$, quand $a \neq 0$.
Donc d contient $p^n + 1$ points : $\mathbb{P}$ est bien d'ordre p^n □

Conclusion

On a pu ainsi exhiber une construction de certains plans projectifs, notamment ceux d'ordre une puissance d'un nombre premier. Ces objets mathématiques sont d'une extrême importance dans le codage et la cryptographie, et permettent également d'optimiser les plans d'expérimentation empirique.

Références

[1] B Doyle, B Voce, WC Lim et CH Lo : Finite projective geometry 2nd year group project. 2015. `https://www.homepages.ucl.ac.uk/~ucahbdo/FiniteProjectivePlanes.pdf`.

[2] Markus Höglin : The what, how and why of finite projective planes. 2021. `https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9067379&fileOId=9067380`.

[3] Xavier Gourdon : *Les maths en tête : Algebre.* Ellipses, 1994.

[4] Johan Kåhrström : On projective planes. *Techn. Rep*, 2002.