Promenade en géométrie finie

Fabien NARBONNE

Septembre 2023

Ce document est en chantier et devrait être actualiser de temps en temps! N'hésitez pas à m'envoyer des corrections ou des suggestions d'amélioration!
Dernière actualisation : 11 mai 2025

Merci à Mimi pour ses relectures précises et les nombreuses améliorations qu'il m'a suggéré!

Table des matières

Introduction

Jeu de Dooble

Il existe un jeu aux propriétés mathématiques surprenantes : le jeu de Dooble. Ce jeu possède 57 cartes [1] qui possèdent chacune 8 symboles. La propriété remarquable de ce jeu est que chaque paire de carte a exactement un symbole en commun, ni plus ni moins ! On peut s'amuser à chercher sur les trois cartes apparentes de la Figure 1 quels symboles elles ont en commun deux à deux [2]. Il existe alors différentes variantes permettant de jouer au jeu. L'une d'elle consiste à distribuer les cartes aux joueuses et à en laisser une face visible au centre de la table. Chaque joueuse devra alors se débarrasser le plus rapidement de son tas de carte en identifiant le symbole en commun avec la carte au centre et en remplaçant cette dernière avec la sienne. Ajoutons que, si le jeu de Dooble était complet, une autre propriété intéressante est que pour chaque paire de symbole il existerait une unique carte sur lesquels ils figurent.

FIGURE 1 – Jeu de Dooble

Que ce soit à des fins récréatives ou purement cogitatoires on peut se demander s'il existe des variantes de ce jeu avec

1. Un nombre de cartes différent
2. Un nombre de symboles par carte différent
3. Si pour un même nombre de cartes et de symboles il existe deux jeux de Dooble différents. C'est-à-dire qu'on ne peut obtenir l'un à partir de l'autre en changeant simplement les symboles.

Le tableau 2 résume l'état des connaissances actuelles sur ces questions là (la ligne rouge correspondant au jeu de Dooble). La première colonne représente le nombre diminué de 1 de symbole par cartes, aussi appelé l'*ordre* du jeu. La colonne suivante indique le nombre de jeu différents qui peuvent être construits pour un ordre donné et les deux dernières indiquent respectivement le nombre de cartes qu'auraient un tel jeu et le nombre symboles au total. Pour un tableau plus complet voir `https://ericmoorhouse.org/pub/planes/`.

Lien avec la géométrie finie

Aussi surprenant que cela puisse paraître ce qui va nous permettre de répondre à certaines de ces questions combinatoires est la géométrie ! Commençons par changer de vocabulaire pour y voir plus clair et nommons les cartes « droites » et les symboles des « points ». Si un symbole est sur une carte on dira alors que la droite correspondante passe par le point. On peut alors reformuler les propriétés de notre jeu de la façon suivante :

1. « *Chaque droite possède le même nombre de points.* »
2. « *Par tout couple de points passe une seule droite.* »
3. « *Chaque paire de droites se croise en un même point.* »

1. En réalité le jeu original ne possède que 55 cartes pour des raisons qui me sont inconnues pourtant il devrait en posséder 57. Il en manque 2.
2. Réponse : Le clown pour les deux cartes du bas, le point d'interrogation pour celle de gauche et celle du haut et l'ancre pour la dernière paire.

Nombre de symboles par carte −1	Nombre de jeux différents	Nombre de cartes au total	Nombre de symbole au total
2	1	7	7
3	1	13	13
4	1	21	21
5	1	31	31
6	0	43	43
7	1	57	57
8	1	73	73
9	4	91	91
10	0	111	111
11	1	133	133
12	?	157	157

FIGURE 2

Énoncé de cette manière, on l'aura reconnu, il s'agit de la géométrie projective plane! Cette dernière ressemble à la géométrie affine plane à l'exception près qu'en géométrie projective plane toutes les droites se croisent, i.e. il n'existe pas de droites parallèles.

Objectifs de ce document

L'objectif de ce document est de présenter des résultats élémentaires de géométrie plane et d'explorer le tableau de la Figure 2 à l'aide d'outils les plus élémentaires possibles.

Objectifs réalisés

Un des objectifs que je souhaitais réaliser était une preuve de l'existence de deux plans projectifs non isomorphes d'ordre 9. C'est à dire prouver qu'il existe deux jeux de Dooble ayant chacun 10 symboles par carte et qu'on ne peut obtenir un jeu à partir de l'autre simplement en changeant les symboles.

Objectifs à réaliser

Voici la liste des objectifs que je souhaite réaliser dans ce document :

- Prouver à l'aide d'outils élémentaires qu'il n'existe pas de plan projectif d'ordre 6, i.e. qu'il n'existe pas de jeu de Dooble dont le nombre de symboles par carte est 7 ou de façon équivalente qu'il n'existe pas de jeu de Dooble à 43 cartes. Ce résultat est une conséquence du Théorème de Bruck-Ryser que s'il existe un plan projectif d'ordre q de la forme $q = 1 \mod 4$ ou $q = 2 \mod 4$ alors q est somme de deux carrés. Ainsi, s'il existait un plan projectif fini d'ordre 6 alors 6 serait somme de deux carrés d'entier ce qui n'est pas le cas.

Structure du document

Dans la Section 1 de ce document nous allons définir de façon axiomatique les plans projectifs finis ainsi que les plans affines finis. Nous étudierons alors ces deux objets. Nous montrerons que si un plan

projectif d'ordre d, i.e. ayant toutes ses droites de cardinal $d+1$, alors il possède d^2+d+1 points (Théorème 1) que si les droites d'un plan affine ont d points alors ce dernier a d^2 points (Théorème 2). Enfin nous définirons des morphismes de plans. On comprendra alors notamment pourquoi la 3-ème et la quatrième colonne de ce tableau sont identiques, i.e. pourquoi un jeu de Dooble doit posséder autant de symboles que de cartes ou, en langage géométrique, pourquoi un plan projectif fini doit avoir autant de points que de droites.

Dans la Section 2 nous tenterons de tisser des liens entre les plans projectifs et les plans affines. Nous verrons que l'on peut construire un unique plan projectif de cardinal d^2+d+1 à partir d'un plan affine de cardinal d^2 en lui rajoutant une droite et que, réciproquement, on peut construire des plans affines à partir des plans projectifs en leur retirant une droite.

Dans la Section 3 nous définirons des sous-ensembles du groupe symétrique $\mathfrak{S}_d$ appelés des *pelotes*. Il existe une certaine dualité entre ces objets et les plans affines finis. De plus on montrera que deux plans affines sont isomorphes si et seulement si leurs pelotes associées sont conjuguées l'une de l'autre.

Dans la Section 4 on définira de nouveaux plans affines appelés *plans de Moulton* d'ordre q^2 pour q une puissance d'un entier impair.

Enfin, dans la Section 5, grâce aux résultats sur les pelotes on montrera que ces plans affines ne sont pas isomorphes aux plans affines canoniques issus de la structure affine de $(\mathbb{F}_{q^2})^2$.

1 Plans finis

Définition 1. *Soit P un ensemble fini de cardinal m et $\mathscr{D} \subseteq \mathscr{P}(P)$ composé de sous-ensembles de P. Deux éléments $D, D' \in \mathscr{D}$ sont dits* parallèles *lorsque $D \cap D' = \emptyset$. On considère les axiomes suivants :*

Axiome 1 : *Tous les éléments de $\mathscr{D}$ sont de même cardinal > 1.*

Axiome 2 : *Pour tout couple d'éléments $x \neq y \in P$ il existe un unique $D \in \mathscr{D}$ tel que $x, y \in D$.*

Axiome 3 : *Pour tout $D \neq D' \in \mathscr{D}, D \cap D' = \{x\}$ pour un élément $x \in P$.*

Axiome 3' : *Il existe $D \in \mathscr{D}$ et $x \notin D$ tel qu'il existe exactement une parallèle D' à D telle que $x \in D'$.*

Les éléments de $\mathscr{D}$ sont alors appelés droites *de P et puisqu'une droite D est déterminée par deux de ses points on pourra noter $D = (xy)$ si $x \neq y \in D$.*

Plans projectifs finis : *Un couple $(P, \mathscr{D})$ vérifiant les axiomes (1), (2) et (3) et tel qu'il existe 4 points distincts de P dont 3 ne sont pas alignés est appelé un* plan projectif fini. *L'entier d tel que toutes les droites sont de cardinal $d+1$ est appelé l'*ordre [3] *du plan projectif.*

Plans affines finis : *Un couple $(P, \mathscr{D})$ vérifiant (1), (2) et (3') est appelé un* plan affine fini. *L'entier d tel que toutes les droites sont de cardinal d est appelé l'*ordre *du plan affine.*

Remarque 1.

1. *Le fait d'exiger qu'il existe 4 points dont 3 ne sont pas alignés permet d'éviter que le couple d'ensembles $(P, \mathscr{D})$ avec $P = \{A, B, C\}$ et $\mathscr{D} = \{\{A, B\}, \{A, C\}, \{B, C\}\}$ ne soit considérer comme un plan projectif. En effet, ce dernier satisfait les 3 premiers axiomes mais on ne peut pas créer son dual affine comme on souhaite le faire dans la Section 2 car ne dernier n'aurait qu'un point et une droite qui possèderait un seul point et contradirait donc le premier axiome.*
2. *L'axiome (3) est implique l'inexistence de droites parallèles.*

3. Le fait de considérer ce $d+1$ au lieu de d permet d'obtenir des plans projectifs et affine de même ordre par dualité.

3. *Concernant la définition des plans affines finis on est obligé de forcer le nombre de parallèles passant par un point à être au plus* 1 *pour éviter les ensembles qui ressemblent à des* $(\mathbb{F}_q)^n$ *dont la géométrie ne ressemblera pas du tout à la géométrie plane.*
   Par exemple, dans $\mathbb{F}_2^3$ *chaque droite* D *admet* 3 *parallèles passant par tout point* x *qui n'est pas sur* D.

Exemple 1. *Pour tout corps fini* $\mathbb{F}_q$ *le couple* $\left(\mathbb{P}^2(\mathbb{F}_q), \mathscr{D}\right)$ *avec* $\mathscr{D}$ *l'ensemble des droites de* $\mathbb{P}^2(\mathbb{F}_q)$ *est un plan projectif fini.*

Exemple 2. *On peut se demander s'il existe des plans projectifs finis* $P = \{\alpha, \beta, \gamma, \delta\}$ *à* 4 *éléments. Si tel est le cas ses droites devraient avoir* 2 *ou* 3 *points. Si les droites ont* 2 *points alors les droites* $(\alpha\beta)$ *et* $(\gamma\delta)$ *existent par le second axiome et ne s'intersectent pas. Si les droites ont* 3 *points alors on peut supposer que* $D = \{\alpha, \beta, \gamma\}$ *est une droite. La droite* $D'(\delta\alpha)$ *possédant un troisième point disons* β *alors* α *et* β *sont traversés par deux droites distinctes ce qui contredit le second axiome. Il n'existe donc pas de plan projectif fini de cardinal* 4.

Exemple 3. *Soit* R *un anneau commutatif fini. Alors le couple* $(R^2, \mathscr{D})$ *avec*

$$\mathscr{D} = \left\{\left\{(x,y)/\, ax+by+c\right\}, (a,b,c) \in R^3 \setminus \{0\}\right\}$$

est un plan affine fini si et seulement si R *est intègre.*

$\boxed{\Leftarrow}$ *Si* R *intègre, commutatif et fini alors* R *est un corps donc* R^2 *est l'espace affine classique.*

$\boxed{\Rightarrow}$ *Si* R *non intègre alors on pose* $a \neq 0$ *un diviseur de zéro et* $b \neq 0$, $ab = 0$. *Alors la droite* $y = ax$ *rencontre* $y = 0$ *en deux points distincts* $(0,0)$ *et* $(b,0)$ *ce qui contredit le second axiome.*

1.1 Plans projectifs finis

Théorème 1. *Soit* $(P, \mathscr{D})$ *un plan projectif fini avec* $\#P = m$ *d'ordre* d. *Alors*

1. d *divise* $m-1$ *et chaque point est traversé par* $\frac{m-1}{d}$ *droites.*
2. *On a* $m = d^2 + d + 1$.
3. $\#\mathscr{D} = m = d^2 + d + 1$.

Démonstration.

1. Soit $x \in P$ et k_x le nombre de droites qui traversent x. D'après le second axiome l'application suivante est bien définie
$$\begin{array}{rccc} \varphi\colon & P\setminus\{x\} & \longrightarrow & \mathscr{D} \\ & y & \longmapsto & (xy) \end{array}$$
   Puisqu'il s'agit d'ensembles fini on a $\#P \setminus \{x\} = \sum_{D\in\mathscr{D}} \#\varphi^{-1}\{D\}$. Ceci donne $m-1 = k_x \cdot d$.
2. Soit D une droite quelconque et $x \notin D$. On pose $\mathscr{D}_x$ l'ensemble des droites contenant x. Alors l'application
$$\begin{array}{rccc} \varphi\colon & D & \longrightarrow & \mathscr{D}_x \\ & y & \longmapsto & (xy) \end{array}$$
   est une bijection. En effet, elle est injective car sinon on aurait deux points $y \neq z \in D$ tels que $(xy) = (xz)$, i.e. x, y, z alignés, i.e. $x \in (yz) = D$ absurde. Elle est surjective car toute droite D' passant par x est distincte de D et coupe donc D en un unique point y, i.e. $\varphi(y) = D'$. On en déduit que $d+1 = \frac{m-1}{d}$ donc $m = d^2 + d + 1$.

3. On note $k = \#\mathscr{D}$ le nombre de droites. On calcule $S = \sum_{D\in\mathscr{D}} \#D$ de deux façons différentes. On a bien entendu $S = k(d+1)$. Chaque point étant traversé par $\frac{m-1}{d}$ droites on a aussi $S = \frac{m-1}{d}\cdot m$. D'où $k = \frac{m(m-1)}{d(d+1)} = d^2+d+1$.

□

Définition 2 (Plan projectif fini dual)**.** *On considère $(P,\mathscr{D})$ un plan projectif fini. On pose $(P^*,\mathscr{D}^*)$ avec $P^* = \mathscr{D}$ et $\mathscr{D}^* = P$ où on identifie $x \in P$ avec $\{D \in \mathscr{D} / x \in D\}$ et on pose pour $x \neq y \in \mathscr{D}^*$, $x \cap y = (xy) \in P^*$. Alors $(P^*,\mathscr{D}^*)$ est un plan projectif fini appelé* dual *de $(P,\mathscr{D})$. On a alors bien entendu $((P^*)^*,(\mathscr{D}^*)^*) = (P,\mathscr{D})$.*

Démonstration.

1. L'axiome (1) est satisfait d'après le premier point du Théorème 1.
2. Soient $D, D' \in P^* = \mathscr{D}$. On a donc[4] $D, D' \in x \Leftrightarrow D, D' \in x$, i.e. $x \in D \cap D'$. Mais d'après l'axiome (3) vérifié par $(P,\mathscr{D})$ il existe un unique $x \in P$ vérifiant cette propriété.
3. L'axiome (3) est vérifié pour $(P^*,\mathscr{D}^*)$ car $(P,\mathscr{D})$ vérifie l'axiome (2).

□

1.2 Plans affines finis

Théorème 2. *Soit $(A,\mathscr{D})$ un plan affine fini d'ordre d. Alors*

1. *Chaque point de A est traversé par $\frac{m-1}{d-1}$ droites.*
2. *Pour chaque $x \in A$ et $D \in \mathscr{D}$ telle que $x \notin D$ il existe une unique parallèle à D passant par x.*
3. *$\#A = d^2$*
4. *$\#\mathscr{D} = d(d+1)$.*

Démonstration.

1. La preuve de la première assertion du Théorème 1 n'utilise que les axiomes (1) et (2) donc reste vraie en affine. Donc le nombre de droites passant par x est $\frac{m-1}{d-1}$.
2. On pose D une droite et $x \notin D$. On considère l'application

$$\begin{array}{rccc} \varphi_x : & D & \longrightarrow & \mathscr{D}_x \\ & y & \longmapsto & (xy) \end{array}$$

   qui est une injection et définie une bijection sur l'ensemble des droites passant par x non parallèles à D. Donc, d'après le point précédent, en notant $p_{D,x} \in \{0,1\}$ le nombre de parallèles à D passant par x, on a $d = \frac{m-1}{d-1} - p_{D,x}$. On en déduit que $p = p_{D,x} = d - \frac{m-1}{d-1}$ qui ne dépend pas de x ni de D. Puisqu'au moins une droite admet exactement une parallèle on a $p = 1$.
3. D'après la preuve de l'assertion précédente chaque point est bien traversé par $\frac{m-1}{d-1}$ droites et on a $\frac{m-1}{d-1} - 1 = d$ donc $m = d^2$ avec $m = \#A$.
4. Pour $\#\mathscr{D} = d(d+1)$, exactement la même preuve que le point 3 du Théorème 1 fonctionne aussi.

□

On a aussi ce corollaire qui justifie le fait que la relation "être parallèle ou égale" est une relation d'équivalence

4. On rappelle qu'on identifie $x \in \mathscr{D}^*$ avec l'ensemble des droites qui traversent x.

Corollaire 1. *Soit $(A,\mathscr{D})$ un plan affine fini. Soit D_1,D_2,D_3 trois droites distinctes de $\mathscr{D}$. Supposons que D_1 et D_2 sont parallèles et que D_2 et D_3 sont parallèles. Alors D_1 et D_3 sont parallèles.*

Démonstration. Supposons que D_1 et D_3 ne soient pas parallèles. Alors il existe $x \in D_1 \cap D_3$ mais alors D_2 possède deux parallèles passant par le point x ce qui contredit l'unicité énoncée dans le second point du Théorème 2. □

Définition 3 (Direction d'une droite)**.** *Soit $(A,\mathscr{D})$ un plan affine fini. D'après le Corollaire 1 la relation être parallèle ou égale définit une relation d'équivalence $\sim$ sur $\mathscr{D}$. On appelle* direction *d'une droite $D \in \mathscr{D}$ sa classe dans le quotient $\mathscr{D}/\sim$ notée $\overrightarrow{D}$.*

Proposition 1. *Soit $(A,\mathscr{D})$ un plan affine fini. Soit $\delta \in \mathscr{D}/\sim$ une direction alors*

$$A = \bigsqcup_{D \in \mathscr{D}/\overrightarrow{D}=\delta} D.$$

En particulier, $\left\{D \in \mathscr{D}/\overrightarrow{D} = \delta\right\} = d$.

Démonstration. Lorsque l'on considère des droites $D_1,\dots,D_r$ toutes parallèles deux à deux alors leur unions est disjointe. On part d'une droite D_1 de direction δ puisque $\#D_1 = d < d^2 = \#A$ il existe $x_1 \in A \setminus D_1$. On considère D_2 l'unique droite parallèle à D_1 passant par x_1. On a alors $\#(D_1 \cup D_2) = 2d$. On suppose construites r droites $D_1, D_2, \dots, D_r$ parallèles deux à deux. Leur union est de cardinal rd. Tant que $rd < d^2$, i.e. $r < d$ il existe $x_{r+1} \in A \setminus (D_1 \cup \dots \cup D_r)$ de telle sorte qu'il existe D_{r+1} passant par x_{r+1} et parallèle à D_1 donc à D_i pour $i \leq r$ d'après le Corollaire 1. □

Corollaire 2. *Soit $(A,\mathscr{D})$ un plan affine fini alors*

$$\#(\mathscr{D}/\sim) = d+1.$$

Démonstration. On considère la surjection canonique

$$\begin{array}{rccc} \pi\colon & \mathscr{D} & \longrightarrow & \mathscr{D}/\sim \\ & D & \longmapsto & \overrightarrow{D}. \end{array}$$

Comme d'habitude, $\mathscr{D}$ est partitionné par les préimages des singletons par π, i.e.

$$d(d+1) = \#\mathscr{D} = \sum_{\delta \in \mathscr{D}/\sim} \underbrace{\#\pi^{-1}(\delta)}_{=d}.$$

□

Proposition 2. *Soit A un ensemble fini de d^2 éléments avec $d \geq 2$, et $\mathscr{D} \subseteq \mathscr{P}(A)$. On suppose que*

1. *$\forall D \in \mathscr{D}, \#D = d$,*
2. *$\mathscr{D} = \bigsqcup_{i=1}^{d+1} \delta_i$ avec $\forall i, \delta_i$ sous-ensemble de $\mathscr{D}$ de cardinal d,*
3. *$\forall 1 \leq i \leq d+1, \forall D \neq D' \in \delta_i, D \cap D' = \emptyset$,*
4. *$\forall D, D' \in \mathscr{D}, \#\left(D \cap D'\right) \leq 1$.*

Alors $(A,\mathscr{D})$ est un plan affine fini.

Démonstration. L'axiome 1 et $3'$ sont tous deux vérifiés par les hypothèses 1 et, 2 et 3. Il reste à vérifier que l'axiome 2 est vérifié. On pose $(\mathscr{D}/\sim) = \{\delta_1, \ldots, \delta_{d+1}\}$ appelé l'ensemble des directions de A. On remarque que pour tout $1 \leq i \leq d+1, \bigcup_{D \in \delta_i} D$ est une partition de A. En effet, l'union est disjointe donc c'est un sous-ensemble de cardinal d^2 de A donc c'est exactement A. Pour tout point $z \in A$ et $\delta \in \mathscr{D}/\sim$, $\exists! D \in \delta | z \in D$. On note δ_z cette droite. On en déduit aussi que toute droite de direction différente se croise en un unique point. En effet, si $D \in \delta, D' \in \delta'$ avec $\delta \neq \delta'$ par tout point de D passe une droite distincte de δ' et D a d point et δ' possède d droites dont D'. Soient $x \neq y \in A$. On veut montrer qu'il existe une unique droite qui passe par x et y. L'unicité est assurée par l'hypothèse 4.

On fixe δ un élément quelconque de $\mathscr{D}/\sim$ et δ_y la droite de δ passant par y. Si elle contient x on a terminé. Sinon, on pose alors

$$\begin{array}{rl} (\mathscr{D}/\sim) \setminus \{\delta\} & \longrightarrow \delta_y \\ \delta' & \longmapsto \delta'_x \cap \delta_y \end{array}$$

qui est injective car les droites de δ' ne se croisent pas. Elle est donc aussi surjective car l'ensemble de départ et d'arrivée sont de même cardinal. Donc il existe une direction dont une droite contient x et y. □

1.3 Morphismes de plans finis

Dans cette section on définit la notion de morphisme de plans qui nous permettra de comparer des plans entre eux.

Définition 4 (Morphismes de plans finis)**.** *Soient $(E, \mathscr{D})$ et $(E', \mathscr{D}')$ deux plans finis (projectif ou affine). Un* morphisme de plans finis *est une application $f : E \longrightarrow E'$ telle que $\forall D \in \mathscr{D}, \exists D' \in \mathscr{D}' / f(D) \subseteq D'$.*

On dit que $(E, \mathscr{D})$ et $(E', \mathscr{D}')$ sont isomorphes si, et seulement s'il existe $f : E \to E'$ et $g : E' \to E$ deux morphismes tels que $f \circ g = \mathrm{id}_{E'}$ et $g \circ f = \mathrm{id}_E$.

Définition 5 (Morphismes séparants/proprement séparants)**.** *Soient $(E, \mathscr{D})$ et $(E', \mathscr{D}')$ deux plans finis. On dit qu'un morphisme de plans finis $f : (E, \mathscr{D}) \to (E', \mathscr{D}')$ est* séparant *lorsque $\forall D \in \mathscr{D}, \exists! D' \in \mathscr{D}'$ telle que $f(D) \subseteq D'$. En particulier, f induit une application*

$$\begin{array}{rccl} f_{\mathscr{D}} : & \mathscr{D} & \longrightarrow & \mathscr{D}' \\ & D & \longmapsto & D' \text{ telle que } f(D) \subseteq D' \end{array}$$

On dit que f est proprement séparant *lorsque f est séparant et $\forall D, D' \in \mathscr{D}, f(D \cap D') = f_{\mathscr{D}}(D) \cap f_{\mathscr{D}}(D')$. En particulier, un morphisme proprement séparant respecte le parallélisme.*

Les morphismes injectifs sont toujours séparant car pour tout $x, y \in A$ et pour toute droite $D' \in \mathscr{D}'$ telle que $f((xy)) \subseteq D'$ on a $f(x), f(y) \subseteq D'$ donc $D' = (f(x)f(y))$ bien définie car $f(x)$ et $f(y)$ sont distincts.

Exemple 4. *Soit $s \geq 1$ un entier et q une puissance de nombre premier $\mathbb{F}_q^2 \hookrightarrow \mathbb{F}_{q^s}^2$ l'inclusion canonique. Est un morphisme de plans affines finis proprement séparant car deux droites affines non verticales sont parallèles si et seulement si elles ont la même pente et une ordonnée à l'origine distincte ce qui ne change pas quand on les injecte dans $\mathbb{F}_{q^s}^2$. De même l'intersection de deux droites paramétrées par des éléments de $\mathbb{F}_q$ a son intersection dans $\mathbb{F}_q$ si elle en a une.*

Exemple 5. *L'inclusion canonique*

$$\begin{array}{rcl} \mathbb{F}_q^2 & \hookrightarrow & \mathbb{P}^2(\mathbb{F}_q) \\ (x, y) & \longmapsto & [x : y : 1]. \end{array}$$

est un morphisme de plans finis séparant.

Exemple 6. *On considère $\mathbb{F}_2^2$ muni de sa structure affine canonique. Alors, pour toute application $\mathbb{F}_2^2 \to (A, \mathscr{D})$ est un morphisme de plans finis.*

Si on considère le cas particulier où $(A, \mathscr{D})$ est $\mathbb{F}_3^2$ muni de sa structure affine canonique et $\mathbb{F}_2^2 \hookrightarrow \mathbb{F}_3^2$ est induit par l'injection $0_{\mathbb{F}_2} \mapsto 0_{\mathbb{F}_3}$ et $1_{\mathbb{F}_2} \mapsto 1_{\mathbb{F}_3}$ alors c'est un morphisme séparant car injectif mais n'est pas proprement séparant car les droites $y = x$ et $y = 1 - x$ sont parallèles dans $\mathbb{F}_2^2$ mais se croisent en $(-1, -1)$ dans $\mathbb{F}_3^2$ donc l'injection ne respecte pas le parallélisme.

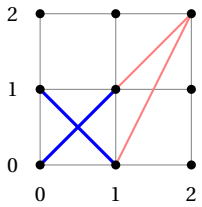


FIGURE 3 – En bleu l'image de la diagonale et de l'antidiagonale de $\mathbb{F}_2^2$ et en rouge les droites de $\mathbb{F}_3^2$ qui les prolongent

Proposition 3. *Soient $(E, \mathscr{D})$ et $(E', \mathscr{D}')$ deux plans finis et $f : E \to E'$ une application. Alors les propositions sont équivalentes :*

1. *f est un isomorphisme.*
2. *$f : E \longrightarrow E'$ est un morphisme bijectif.*
3. *f induit une application bijective*
$$\begin{array}{ccc} \mathscr{D} & \longrightarrow & \mathscr{D}' \\ D & \longmapsto & f(D) \end{array}$$

Dans ce cas E et E' sont tous les deux affines ou tous les deux projectifs et f est proprement séparant.

Démonstration. On commence par prouver que s'il existe une bijection $E \to E'$ ou $\mathscr{D} \to \mathscr{D}'$ alors $(E, \mathscr{D})$ et $(E', \mathscr{D}')$ sont tous les deux projectifs ou tous les deux affines et $d = d'$ (avec d, d' les ordres des deux plans).

On suppose que $f : E \to E'$ morphisme bijectif. D'après la section précédente qu'ils soient projectifs où affines le cardinal d'un plan fini est déterminé par le nombre de point par droite. Supposons par l'absurde que l'un soit affine de cardinal d^2 et l'autre projectif de cardinal $d'^2 + d' + 1$. On a alors $d^2 = d'^2 + d' + 1$, i.e. en passant à la forme canonique

$$\left(d - d' - \frac{1}{2}\right)\left(d + d' + \frac{1}{2}\right) = \frac{3}{4} \Leftrightarrow \left(2d - 2d' - 1\right)\left(2d + 2d' + 1\right) = 3$$

donc $2d - 2d' - 1 = 1$ et $2d + 2d' + 1 = 3$ ce qui implique $d = 1$ absurde.

Donc E et E' sont du même type et donc ont le même nombre de points par droite (car $d \mapsto d^2$ et $d \mapsto d^2 + d + 1$ sont injectives sur $\mathbb{R}^+$).

On prouve de la même façon que s'il existe une bijection $\mathscr{D} \to \mathscr{D}'$ alors $(E, \mathscr{D})$ et $(E', \mathscr{D}')$ sont de même type. En effet, si ce n'était pas le cas on aurait une égalité de la forme $d^2 + d = d'^2 + d' + 1$ ce qui est impossible car l'entier de gauche est pair et celui de droite est impair.

(1) $\Longrightarrow$ (2) : Évident.

(2) $\Longrightarrow$ (1) : On pose $g = f^{-1}$. Soit $D \in \mathscr{D}$ et $D' \in \mathscr{D}'$ telle que $f(D) \subseteq D'$. Le morphisme f réalise donc une injection de D vers un ensemble de même cardinal c'est donc une bijection d'inverse ψ. Soit $D' \in \mathscr{D}'$ et x', y' deux points distincts de D'. Soient $x = f^{-1}(x')$, $y = f^{-1}(y')$ distincts et $D = (xy) \in \mathscr{D}$ alors $f(D) = D''$ avec $D'' \in \mathscr{D}$ et $x', y' \in D''$ donc $D'' = D'$. On a donc bien $g(D') = D \in \mathscr{D}$ et donc g est bien un morphisme.

(2) $\Longleftrightarrow$ (3) : La preuve de (2) $\Rightarrow$ (1) prouve (2) $\Rightarrow$ (3). Maintenant, supposons (3). Par hypothèse, f est un morphisme. Soit $x \neq y \in D \in \mathscr{D}$ alors $f((xy)) = D'$ pour une certaine droite $D' \in \mathscr{D}'$. Puisque $d = d'$ et que $f_{|D}$ est surjective entre deux ensembles de même cardinal alors elle est aussi injective donc $f(x) \neq f(y)$ donc f est injective entre deux ensembles de mêmes cardinaux donc elle est bijective.

□

Corollaire 3. *Soit $f : (A, \mathscr{D}) \longrightarrow (A', \mathscr{D}')$ un isomorphisme de plans affines. Alors, la bijection $\mathscr{D} \to \mathscr{D}'$ induite par f passe au quotient modulo $\sim$, i.e. f envoie des droites parallèles sur des droites parallèles.*

Démonstration. Soient $D_1, D_2 \in \mathscr{D}$ parallèles alors, puisque f est une bijection,

$$f(D_1 \cap D_2) = f(\emptyset) = \emptyset = f(D_1) \cap f(D_2)$$

donc $f(D_1)$ et $f(D_2)$ sont parallèles. □

2 Dualité partielle affine-projectif

2.1 Projectivisation des plans affines

Dans cette partie on souhaite construire un plan projectif d'ordre d à partir d'un plan affine d'ordre d et prouver que cette construction est unique à isomorphisme près.

Théorème 3. *Soit $(A, \mathscr{D})$ un plan affine fini d'ordre d alors il existe un plan projectif fini $(\overline{A}, \overline{\mathscr{D}})$ d'ordre d et un morphisme injectif $(A, \mathscr{D}) \hookrightarrow (\overline{A}, \overline{\mathscr{D}})$.*

De plus $(\overline{A}, \overline{\mathscr{D}})$ est unique à isomorphisme près, i.e. pour toute injection $(A, \mathscr{D}) \hookrightarrow (P, \mathscr{D}')$ où $(P, \mathscr{D}')$ est un plan projectif d'ordre d alors $(P, \mathscr{D}') \simeq (\overline{A}, \overline{\mathscr{D}})$. Le plan $(\overline{A}, \overline{\mathscr{D}})$ est alors appelé le projectivisé *de $(A, \mathscr{D})$.*

Démonstration. Soit $(A, \mathscr{D})$ un plan affine fini d'ordre d. D'après le Théorème 2, $\#\mathscr{D} = d(d+1)$. On pose $\overline{A} = A \sqcup \{\delta_1\} \sqcup \cdots \sqcup \{\delta_{d+1}\}$, avec $\mathscr{D} / \sim = \{\delta_1, \ldots, \delta_{d+1}\}$, i.e. on rajoute formellement les $d+1$ directions à A que l'on appelle *points à l'infini*. On pose pour tout D telle que $\overrightarrow{D} = \delta, \overline{D} = D \sqcup \{\delta\}$ et $D_\infty = \{\delta_1, \ldots, \delta_{d+1}\}$ que l'on appelle *droite à l'infini* ou *horizon* de A. Enfin, on définit

$$\overline{\mathscr{D}} = \left\{\overline{D}, D \in \mathscr{D}\right\} \cup \{D_\infty\}.$$

On vérifie que les 3 axiomes sont bien vérifiés pour $(\overline{A}, \overline{\mathscr{D}})$.

Axiome 1 : Les droites ont bien toutes $d+1$ (on ajoute 1 point aux droites affines et $\#D_\infty = d+1$).

Axiome 2 : Soient $x \neq y \in \overline{A}$.

- Si x, y sont tous les deux à l'infini alors la seule droite qui les contient est D_∞ car toute droite issue de droite affine contient exactement 1 point à l'infini.
- Si $x, y \in A$ alors, par le deuxième axiome, $\exists! D = (xy) \in \mathscr{D}$ qui passe par x et y. Il est clair que c'est toujours la seule droite qui vérifie cette propriété.

- Si x affine et $y = \delta$ à l'infini alors il existe une unique droite D de direction δ qui passe par x et on a $x, y \in \overline{D}$ par définition. Les autres droites affines passant par x ne sont pas parallèle à D donc sont complétées par un autre point que y à l'infini. Enfin, $x \notin D_\infty$.

Axiome 3 : Soient $D \neq D' \in \overline{\mathscr{D}}$ deux droites.

- Si D et D' sont issues de droites affines de même direction δ alors elles n'ont pas d'intersection affine par définition mais elles se croisent en δ.
- Si D et D' sont issues de droites affines de direction différentes alors elles admettent une unique intersection affine par définition et leurs points à l'infini sont différents.
- Si D est issue d'une droite affine et $D' = D_\infty$. Alors $D \cap D' = \{x_i\}$ avec $\overrightarrow{D} = \delta_i$.

On montre maintenant l'unicité. Soit $\iota\colon (A, \mathscr{D}) \to (\overline{A}, \overline{\mathscr{D}})$ l'injection qu'on vient de mettre en valeur et soit $f\colon (A, \mathscr{D}) \to (P, \mathscr{D}')$ une autre injection vers un plan projectif d'ordre d. On veut définir une application $\Phi\colon (P, \mathscr{D}') \to (\overline{A}, \overline{\mathscr{D}})$. Pour tout $y \in f(A)$ on pose $\Phi(y) = \iota(f^{-1}(y))$ (f réalise un isomorphisme sur son image). Il reste $y_1, \dots, y_{d+1} \in P \setminus f(A)$ pour lesquels on doit définir l'image par Φ. On les appelles les points à l'infini.

On remarque que, puisque f est injective, elle est séparante et donc induit une application $\widetilde{f}\colon \mathscr{D} \to \mathscr{D}'$ définie par $\forall x \neq y \in A, f((xy)) = (f(x)f(y))$. Chaque droite de P étant de cardinal $d+1$ on a pour tout $D \in \mathscr{D}, \widetilde{f}(D) = f(D) \cup \{y_i\}$ pour un certain i.

Soient $D, D' \in \delta$ deux droites parallèles de $\mathscr{D}$. On note $\widetilde{f}(D) = f(D) \cup \{y\}$ et $\widetilde{f}(D') = f(D) \cup \{y'\}$. Alors

$$\widetilde{f}(D) \cap \widetilde{f}(D') = \big(f(D) \cup \{y\}\big) \cap \big(f(D') \cup \{y'\}\big) = \underbrace{f(D \cap D')}_{=\emptyset} \cup \big(\{y\} \cap \{y'\}\big) = \{y\} \cap \{y'\}.$$

Donc, puisque $(P, \mathscr{D}')$ est supposé être un plan projectif, par l'axiome 3, $y = y'$. C'est-à-dire que les images de droites de même direction se croisent en un même point à l'infini. On peut donc définir une application

$$\begin{aligned} \pi\colon \quad \mathscr{D}/\sim = \{\delta_1, \dots, \delta_{d+1}\} &\longrightarrow \{y_1, \dots, y_{d+1}\} \\ \delta &\longmapsto \widetilde{f}(D) \setminus f(D) \text{ pour } D \in \delta. \end{aligned}$$

Soit $\overrightarrow{D}, \overrightarrow{D}' \in \mathscr{D}/\sim$ tels que $\pi\left(\overrightarrow{D}\right) = \pi\left(\overrightarrow{D}'\right) = y$. Si D et D' se croisent en $x \in A$ alors

$$\widetilde{f}(D) = f(D) \cup \{y\} = f(D') \cup \{y\} = \widetilde{f}(D') = (f(x)y).$$

Donc $D = D'$ donc $\delta = \delta'$, i.e. π est injective et on peut supposer que $\pi(\delta_i) = y_i$ quitte à réordonner les y_i.

On rappelle que $\overline{A} = A \sqcup \{\delta_1, \dots, \delta_{d+1}\}$ avec δ_i considéré comme point d'intersection de toutes les droites $\overline{D} = D \sqcup \{\delta_i\}$ telles que $\overrightarrow{D} = \delta_i$ une direction. On pose donc $\Phi(y_i) = \delta_i$.

Ainsi Φ est une application bijective, il reste à montrer qu'il s'agit d'un morphisme. On remarque que $\widetilde{f}(D) = f(D) \cup \{x\} = \widetilde{f}(D') = f(D') \cup \{x'\}$ implique $x = x'$ et $D = D'$ donc $\widetilde{f}$ est injective donc atteint $d^2 + d$ droites de $\mathscr{D}'$. Il en reste une dernière D_∞ qui n'est pas dans l'image de $\widetilde{f}$. Si D_∞ possédait deux points $f(x), f(y)$ de $f(A)$ alors elle coïnciderait avec $\widetilde{f}(xy)$ et si elle en possédait de la forme $f(x)$ et y_i alors elle coïnciderait avec $\widetilde{f}(D)$ où D est l'unique droite de direction $\pi^{-1}(y_i)$ et passant par x. Donc D_∞ est composée de points à l'infini. Puisqu'il n'y en a que $d+1$ alors $D_\infty = \{y_1, \dots, y_{d+1}\}$.

Soit $D \in \mathscr{D}'$ une droite possédant un point x dans $f(A)$, on pose $y = D \cap D_\infty$. On a alors $D = \widetilde{f}(D_0)$ pour une droite D_0 de direction $\delta = \pi^{-1}(y)$ passant par x. On a donc

$$\Phi(D) = \Phi(f(D_0) \sqcup \{y\}) = \Phi(f(D_0)) \sqcup \{\Phi(y)\} = \iota(f^{-1}(f(D))) \sqcup \{x\} = \iota(D) \sqcup \{x\} = \overline{D} \sqcup \{x\}$$

avec x correspondant à la direction δ. Et Φ envoie bien la droite à l'infini de P sur celle de $\overline{A}$. □

Proposition 4 (Prolongement des morphismes affines séparant)**.** *Soit $(A,\mathscr{D})$ et $(A',\mathscr{D}')$ deux plans affines finis et $f:(A,\mathscr{D})\to(A',\mathscr{D}')$ un morphisme proprement séparant. Alors il existe un unique morphisme $\widetilde{f}$ tel que le diagramme suivant commute*

$$\begin{array}{ccc}(A,\mathscr{D}) & \xrightarrow{f} & (A',\mathscr{D}')\\ \iota\downarrow & & \downarrow\iota'\\ \left(\overline{A},\overline{\mathscr{D}}\right) & \xrightarrow{\tilde{f}} & \left(\overline{A}',\overline{\mathscr{D}}'\right)\end{array}$$

Démonstration. Soit $x\in\iota(A)$ on pose $\widetilde{f}(x)=\iota'(f(\iota^{-1}(x)))$. On rappelle qu'on peut définir $\overline{A}$ par $A\sqcup(\mathscr{D}/\sim)$, le plan affine A auquel on rajoute formellement les directions. On considère maintenant $\delta\in\overline{A}$ une direction vue comme un point de $\overline{A}$. Soient D_1,D_2 deux droites de directions δ. Puisque f et ι' sont séparants on peut définir $y\in\overline{\mathscr{D}}'$ par $(\iota'\circ f)_{\mathscr{D}}(D_1)\cap(\iota'\circ f)_{\mathscr{D}}(D_2)$ (où $(\iota'\circ f)_{\mathscr{D}}$ est l'application qui à une droite D de $\mathscr{D}$ renvoie l'unique de $\overline{\mathscr{D}}'$ qui contient l'image de D par $\iota'\circ f$). Puisque f est proprement séparant $f_{\mathscr{D}}(D_1)$ et $f_{\mathscr{D}}(D_2)$ sont parallèles et donc y se situe à l'infini et ne dépend que de la direction de $f_{\mathscr{D}}(D_1)$ et donc que de la direction de D_1. On a donc une application bien définie $\pi:\mathscr{D}/\sim\to\mathscr{D}'/\sim$ qui permet de prolonger définir $\widetilde{f}$ sur les points à l'infini de $\overline{A}$, i.e. $\widetilde{f}(\delta)=\pi(\delta)$.

On montre que $\widetilde{f}$ préserve l'alignement pour finir de montrer que c'est un morphisme. Puisque $f(\mathscr{D}/\sim)\subseteq\mathscr{D}'/\sim$ et que $D_\infty=\mathscr{D}/\sim$ et $D'_\infty=\mathscr{D}'/\sim$ sont des droites, $\widetilde{f}$ préserve bien l'alignement à l'infini. Soit $\overline{D}=D\sqcup\left\{\overrightarrow{D}\right\}$ une droite de $\overline{\mathscr{D}}$ issue d'une droite affine $D\in\mathscr{D}$. Alors $\widetilde{f}\left(\overline{D}\right)=f_{\mathscr{D}}(D)\sqcup\left\{\widetilde{f}(\delta)\right\}$ avec $\widetilde{f}(\delta)$ la direction de $f_{\mathscr{D}}(D)$ donc c'est bien une droite de $\overline{\mathscr{D}}'$.

Enfin, le fait qu'on n'ait pas eu le choix quant aux images de $\widetilde{f}$ prouve l'unicité. □

2.2 Affinisation des plans projectifs

On souhaite faire la même chose que dans la section précédente pour compléter la dualité affine-projectif. C'est-à-dire qu'étant donné un plan projectif $(P,\mathscr{D})$ d'ordre d on va expliquer comment construire un plan affine $(A,\mathscr{D}')$ à d points à partir de P et muni d'un morphisme injectif $(A,\mathscr{D}')\hookrightarrow(P,\mathscr{D})$. Malheureusement, il n'y a en général pas unicité à isomorphisme près des plans affines contenus dans les plans projectifs.

Théorème 4. *Soit $(P,\mathscr{D})$ un plan affine fini d'ordre d alors il existe un plan affine fini $(P_{\text{aff}},\mathscr{D}_{\text{aff}})$ d'ordre d et une injection $(P_{\text{aff}},\mathscr{D}_{\text{aff}})\hookrightarrow(P,\mathscr{D})$.*

Démonstration. Soit $(P,\mathscr{D})$ un plan projectif d'ordre d. On considère $D_0\in\mathscr{D}$ une droite quelconque qu'on appellera désormais la droite à l'infini. On pose $P_{\text{aff}}=P\setminus D_0$. Soit $D\in\mathscr{D}\setminus\{D_0\}$, on pose $D_{\text{aff}}=D\setminus D_0$ et

$$\mathscr{D}_{\text{aff}}=\left\{D_{\text{aff}},D\in\mathscr{D}\setminus\{D_0\}\right\}.$$

On prouve les 3 axiomes :

Axiome 1 : Les droites ont bien toutes d points (on enlève 1 point aux droites projectives que l'on considère).

Axiome 2 : Soient $x\neq y\in P_{\text{aff}}$. Alors, il existe une unique droite $D=(xy)\in\mathscr{D}$ qui traverse x et y. Puisque $x,y\notin D_0$ par définition de P_{aff} on a bien $x,y\in D_{\text{aff}}$

Axiome 3' : Soit $D\neq D_0$ une droite quelconque de $\mathscr{D}$. Elle rencontre D_0 en un point x_0. Ce point est traversé par $\frac{m-1}{d}=d+1\geq 3$ droites dont D_0 et D donc il existe D' distinct de D_0 et D qui passe aussi par x_0. On pose $x\in D'\setminus\{x_0\}$. On a alors $D_{\text{aff}}\cap D'_{\text{aff}}=(D\cap D')\setminus D_0=\{x_0\}\setminus D_0=\emptyset$, i.e. D'_{aff} est une parallèle à D_{aff} passant par $x'\notin D$.

□

3 Pelotes

3.1 Système de coordonnées affines

Soit $(A, \mathscr{D})$ un espace affine. On pose δ_X et δ_Y deux directions distinctes et D une droite d'une troisième direction. On pose

$$\{X_1, X_2, \ldots, X_d\} = \left\{X \in \mathscr{D} | \overrightarrow{X} = \delta_X\right\}$$
$$\{Y_1, Y_2, \ldots, Y_d\} = \left\{Y \in \mathscr{D} | \overrightarrow{Y} = \delta_Y\right\}$$

Pour tout (i, j), $X_i \cap Y_j = \{x_{ij}\}$ non vide car les droites ne sont pas parallèles et forment des points distincts de A pour $(i, j) \neq (k, \ell)$. En effet, si $X_i \cap Y_j = X_k \cap Y_\ell$ alors $i = k$ et $j = k$ car il s'agit un point commun à X_i, X_k, Y_j et Y_ℓ. On pose $E_d = \{1, 2, \ldots, d\}$. On en déduit que

$$\begin{array}{rl} \mathbb{A}_d = E_d^2 & \longrightarrow A \\ (i, j) & \longmapsto X_i \cap Y_j \end{array}$$

est une injection vers un ensemble de cardinal d^2 donc c'est une bijection. On pose γ son inverse. Ceci nous permet d'identifier A avec l'ensemble $\mathbb{A}_d = E_d^2$ puis, en définissant les droites de $\mathbb{A}_d$ comme les images des droites de A par γ on a muni $\mathbb{A}_d$ d'une structure d'espace affine isomorphe à $(A, \mathscr{D})$.

Enfin, pour D ayant une direction différente de δ_X, pour tout i, on a les intersections $D \cap X_i \neq \emptyset$ et définissent des points distincts car sinon on aurait deux points de D sur un même X_i ce qui imposerait $D = X_i$. De même les $D \cap Y_j$ définissent des points distincts lorsque j varie. Donc, quitte à réordonner les X_i et les Y_j on peut supposer que $\gamma(D) = \{(1, 1), (2, 2), \ldots, (d, d)\}$ appelée la diagonale de $\mathbb{A}_d$.

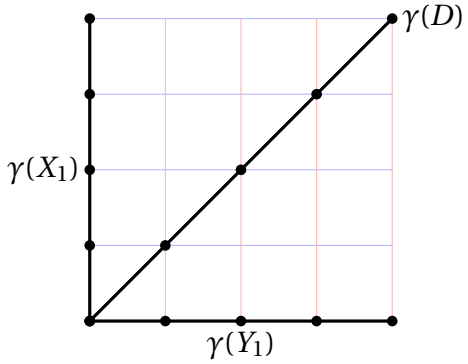


FIGURE 4 – Tout plan affine à 25 éléments peut être représenté comme ci-dessus avec ces $2 \times 5 + 1$ droites

Définition 6 (Plan affine standard)**.** *Soit $E_d = \{1, \ldots, d\}$ et $\mathbb{A}_d = E_d^2$. On dit qu'un plan affine $(\mathbb{A}_d, \mathscr{D})$ est un* plan affine standard *si les ensembles de la forme $Y_j = \{y = j\} = \{(i, j), i \in E_d\}$, $X_i = \{x = i\} = \{(i, j), j \in E_d\}$ et la diagonale $\{(1, 1), (2, 2), \ldots, (d, d)\}$ sont des droites. On dit alors que $(X_i, Y_j)_{1 \leq i, j \leq d}$ sont les coordonnées de $(\mathbb{A}_d, \mathscr{D})$*

Un morphisme de plans affines standards $f : (\mathbb{A}_d, \mathscr{D}) \longrightarrow (\mathbb{A}_d, \mathscr{D}')$ est un morphisme de plans finis tel que $f\left(\overrightarrow{X_1}\right) = \overrightarrow{X_1'}$, $f\left(\overrightarrow{Y_1}\right) = \overrightarrow{Y_1'}$ et $f(D_0) = D_0'$.

D'après ce qui précède tout plan affine fini est isomorphe à un plan affine standard.

Proposition 5. *Soit $f\colon (A,\mathscr{D}) \longrightarrow (A',\mathscr{D}')$ un morphisme de plans affines finis. Alors il existe des plans affines standards $(\mathbb{A}_d,\mathscr{D})$ et $(\mathbb{A}_{d'},\mathscr{D}')$ et deux isomorphismes de plans finis φ et φ' tels que le diagramme suivant commute*

$$\begin{array}{ccc} (A,\mathscr{D}) & \xrightarrow{f} & (A',\mathscr{D}') \\ \varphi\downarrow & & \downarrow\varphi' \\ (\mathbb{A}_d,\mathscr{D}) & \xrightarrow{\widetilde{f}} & (\mathbb{A}_{d'},\mathscr{D}') \end{array}$$

avec $\widetilde{f}$ un morphisme de plans affines standards.

Démonstration. D'après ce qui précède, il existe $\varphi\colon (A,\mathscr{D}) \longrightarrow (\mathbb{A}_d,\mathscr{D})$ un isomorphisme de plans finis. On considère alors $D=\varphi^{-1}(D_0)$ la préimage de la diagonale. Puisque f est un morphisme il existe une droite $D'\in\mathscr{D}'$ telle que $f(D)\subseteq D'$. On choisit alors deux directions $\delta_X,\delta_Y\in\mathscr{D}'/\sim$ distinctes de $\overrightarrow{D'}$ ce qui donne un isomorphisme $\varphi\colon (A',\mathscr{D}')\to(\mathbb{A}_{d'},\mathscr{D}')$ de coordonnées δ_X,δ_Y et de diagonale $\varphi'(D')$. Le morphisme $\widetilde{f}=\varphi'\circ f\circ\varphi^{-1}$ convient. □

3.2 Pelotes du groupe symétrique

On pose $E_d=\{1,\dots,d\}$ et $\mathfrak{S}_d=\mathfrak{S}(E_d)$ le groupe des permutations de E_d. On rappelle que le support d'une permutation $\sigma\in\mathfrak{S}_d$ est défini par

$$\mathrm{Supp}(\sigma)=\{i\in E_d \mid \sigma(i)\neq i\}.$$

Une *pelote* $\mathscr{V}=[V_1,\dots,V_{d-1}]$ de $\mathfrak{S}_d$ est la donnée de d sous-ensembles V_k de $\mathfrak{S}_d$ appelés *directions* de $\mathscr{V}$ tels que :

- $\exists k\in\{1,\dots,d-1\},\mathrm{id}\in V_k$
- $\forall k\in\{1,\dots,d-1\},\#V_k=d$.
- $\forall k\in\{1,\dots,d-1\},\forall\sigma\neq\tau\in V_k,\#\mathrm{Supp}(\sigma\tau^{-1})=d$ (i.e. σ et τ n'ont jamais la même image en un $i\in E_d$).
- $\forall k\neq\ell\in\{1,\dots,d-1\},\forall\sigma\in V_k,\tau\in V_\ell,\#\mathrm{Supp}(\sigma\tau^{-1})=d-1$ (i.e. $\exists! i\in E_d/\sigma(i)=\tau(i)$).

D'autre part on dit que $\forall s\in\mathfrak{S}_{d-1},[V_1,\dots,V_{d-1}]=\left[V_{s(1)},\dots,V_{s(d-1)}\right]$ (l'ordre des V_k n'a pas d'importance).

Deux pelotes $\mathscr{V}=(V_1,\dots,V_{d-1})$ et $\mathscr{V}'=\left(V'_1,\dots,V'_{d-1}\right)$ sont dites *isomorphes* s'il existe $\sigma_0\in\mathfrak{S}_d$ tel que

$$\forall k\in\{1,\dots,d-1\},\sigma_0^{-1}V_k\sigma_0=V'_k$$

à une permutation près des ensembles $V'_2,\dots,V'_{d-1}$.

Théorème 5. *Il existe une bijection entre les plans affines standards $(\mathbb{A}_d,\mathscr{D})$ et les pelotes de $\mathfrak{S}_d$.*

Démonstration. Soit $(\mathbb{A}_d,\mathscr{D})$ un plan affine standard. On pose[5] $\delta_d=\overrightarrow{X_1}$ et $\delta_{d+1}=\overrightarrow{Y_1}$ les directions correspondant aux abscisses et aux ordonnées et $\delta_1,\dots,\delta_{d-1}\in\mathscr{D}/\sim$ les autres directions. Quitte à réordonner les indices on peut supposer que la diagonale D_0 est dans δ_1.

Pour tout $D\in\delta_k$ on pose $\sigma_D\in\mathfrak{S}_d$ tel que $\sigma_D(i)=j$ avec $D\cap X_i=\{(i,j)\}$ (D et X_i ne sont pas parallèles par hypothèse). L'application σ_D est bien un élément de $\mathfrak{S}_d$ car si $\sigma_D(i)=\sigma_D(i')=j$ alors D coupe Y_j en i et i'. Puisque $D\notin\delta_{d+1}$, $i=i'$ (sinon D coïncide avec Y_j en deux points donc $D=Y_j$). On pose $V_k=\{\sigma_D,D\in\delta_k\}$.

5. On considère simplement D comme le graphe d'une permutation.

- On a bien $\mathrm{id} = \sigma_{D_0} \in V_1$.
- Soit $\sigma_D, \sigma_{D'} \in V_k$ et $i \in E_d$. Si $\sigma_D(i) = \sigma_{D'}(i) = j$ alors D et D' s'intersectent en (i,j) puisque δ_k est l'ensemble des droites parallèles ou égales de même direction δ_k on a $D = D'$ donc $\sigma_D = \sigma_{D'}$ donc si $D \neq D' \in \delta_k, \mathrm{Supp}(\sigma_D \sigma_{D'}^{-1}) = E_d$. Ceci prouve aussi que

$$\begin{array}{rl} \delta_k & \longrightarrow V_k \\ D & \longmapsto \sigma_D \end{array}$$

  est bijective donc $\forall k, \#V_k = \#\delta_k = d$.
- Soit $k \neq \ell$ et $\sigma_D \in V_k, \sigma_{D'} \in V_\ell$. Donc les droites D et D' se croisent en un unique point (i,j), i.e. $\sigma_D(i) = \sigma_{D'}(i) = j$ pour un unique point. Donc $\mathrm{Supp}(\sigma_D \sigma_{D'}^{-1}) = E_d \setminus \{i\}$.

Réciproquement, soit $\mathscr{V} = [V_1, \ldots, V_{d-1}]$ une pelote de $\mathfrak{S}_d$. Soit $k \in \{1, \ldots, d-1\}, \sigma \in V_k$ on pose $D_\sigma = \left\{(i,j) \in E_d^2, \sigma(i) = j\right\}$, le graphe de σ et $\delta_k = \{D_\sigma, \sigma \in V_k\}$. On pose $(E_d^2, \mathscr{D}_\mathscr{V})$ avec

$$\mathscr{D}_\mathscr{V} = \bigcup_{k=1}^{d-1} \{D_\sigma, \sigma \in V_k\} \cup \{X_1, \ldots, X_d\} \cup \{Y_1, \ldots, Y_d\}$$

avec $X_i = \left\{(i,j), j \in E_d\right\}, Y_j = \left\{(i,j), i \in E_d\right\}$.

1. Pour toute droite $D = D_\sigma \in \mathscr{D}_\mathscr{V}$ est de cardinal d car bijectivité des élément de $\mathfrak{S}_d$ et c'est immédiat que $\#X_i = \#Y_j = d$ pour tout i, j.
2. Soit $(i,j) \neq (k,\ell) \in E_d^2$.
   - Si $i = k$ alors $j \neq \ell$ et X_i traverse ces deux points. Si D_σ passe par $(i,j), (k,\ell)$ on a $\sigma(i) = j = \ell$ absurde. Donc seule X_i traverse ces deux points.
   - Si $j = \ell$ alors $i \neq k$ et Y_j traverse ces deux points. Si D_σ passe par $(i,j), (k,\ell)$ on a $\sigma(i) = j$ et $\sigma(k) = \ell$ mais, par injectivité de σ on devrait alors avoir $i = k$, absurde. Donc seule Y_j traverse ces deux points.
   - Sinon $i \neq k$ et $j \neq \ell$. Pour $1 \leq \alpha \leq d-1$, on considère

$$\begin{array}{rccl} \gamma_\alpha : & V_\alpha & \longrightarrow & E_d \\ & \sigma & \longmapsto & \sigma(i) \end{array}$$

     Si $\sigma(i) = \tau(i)$ alors $i \notin \mathrm{Supp}(\sigma\tau^{-1})$ absurde car $\mathrm{Supp}(\sigma\tau^{-1}) = E_d$ par hypothèse. Donc γ_α injective et donc surjective. On pose alors σ_α l'unique permutation de V_α telle que $\sigma_\alpha(i) = j$. On considère alors

$$\begin{array}{rccl} \gamma : & \{1, \ldots, d-1\} & \longrightarrow & E_d \\ & \alpha & \longmapsto & \sigma_\alpha(k) \end{array}$$

     Si $\sigma_\alpha(k) = \sigma_\beta(k)$ alors $i, k \notin \mathrm{Supp}(\sigma_\alpha \sigma_\beta^{-1})$ or cet ensemble doit être de cardinal $d-1$ lorsque $\alpha \neq \beta$ i.e.$\sigma_\alpha \neq \sigma_\beta$. Donc γ est aussi injective donc surjective. Donc il existe α tel que $\sigma_\alpha(k) = \ell$ et, par construction $\sigma_\alpha(i) = j$ donc D_{σ_α} passe par (i,j) et (k,ℓ).

3'. Il existe une droite admettant une parallèle car les X_i sont parallèles entre elles.

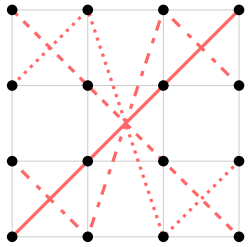
Donc $(E_d^2, \mathscr{D}_\mathscr{V})$ est un plan affine fini.

□

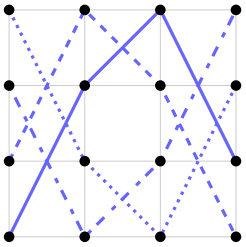
Exemple 7. *L'ensemble $\mathbb{F}_4^2$ muni de la structure d'espace affine issue de sa structure de $\mathbb{F}_4$-espace vectoriel fournit un plan affine fini $(\mathbb{F}_4^2, \mathscr{D})$. On pose $\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{0, 1, \alpha, \alpha+1\}$ avec $\alpha^2 + \alpha + 1 = 0$. On identifie $\mathbb{F}_4$ à $\{1,2,3,4\}$ via la bijection*

$$\begin{array}{rcl} \mathbb{F}_4 & \longrightarrow & \{1,2,3,4\} \\ 0 & \longmapsto & 1 \\ 1 & \longmapsto & 2 \\ \alpha & \longmapsto & 3 \\ \alpha+1 & \longmapsto & 4 \end{array}$$

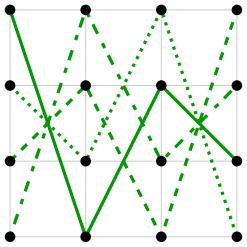
On peut alors identifier $(\mathbb{F}_4, \mathscr{D})$ à un plan affine standard $(A_4, \mathscr{D})$. Les trois directions autres que la direction principale sont les suivantes



(a) Direction Vect$(1,1)$



(b) Direction Vect$(1,\alpha)$



(c) Direction Vect$(1,\alpha+1)$

qui donnent la pelote $\mathscr{V} = [V_1, V_2, V_3]$ de $\mathfrak{S}_4$ suivante

$$\begin{aligned} V_1 &= \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \\ V_2 &= \{(2,3,4), (1,2,4), (1,3,2), (1,4,3)\} \\ V_3 &= \{(2,4,3), (1,2,3), (1,3,4), (1,4,2)\}. \end{aligned}$$

Exemple 8. *Le plan affine canonique sur $\mathbb{F}_9$ donne la pelote suivante :*

$$V_1 = \left\{ \begin{array}{c} \mathrm{id}, \\ (1,2,6)(3,4,9)(5,8,7), \\ (1,3,7)(2,4,5)(6,9,8), \\ (1,4,8)(2,9,7)(3,5,6), \\ (1,5,9)(2,8,3)(4,6,7), \\ (1,6,2)(3,9,4)(5,7,8), \\ (1,7,3)(2,5,4)(6,8,9), \\ (1,8,4)(2,7,9)(3,6,5), \\ (1,9,5)(2,3,8)(4,7,6) \end{array} \right\}, V_2 = \left\{ \begin{array}{c} (2,3,4,5,6,7,8,9), \\ (1,2,4,8,3,9,6,5), \\ (1,3,5,9,4,2,7,6), \\ (1,4,6,2,5,3,8,7), \\ (1,5,7,3,6,4,9,8), \\ (1,6,8,4,7,5,2,9), \\ (1,7,9,5,8,6,3,2), \\ (1,8,2,6,9,7,4,3), \\ (1,9,3,7,2,8,5,4) \end{array} \right\}, V_3 = \left\{ \begin{array}{c} (2,4,6,8)(3,5,7,9), \\ (1,2,9,4)(3,8,6,7), \\ (1,3,2,5)(4,9,7,8), \\ (1,4,3,6)(2,8,9,5), \\ (1,5,4,7)(2,6,3,9), \\ (1,6,5,8)(2,3,7,4), \\ (1,7,6,9)(3,4,8,5), \\ (1,8,7,2)(4,5,9,6), \\ (1,9,8,3)(2,7,5,6) \end{array} \right\}, V_4 = \left\{ \begin{array}{c} (2,5,8,3,6,9,4,7), \\ (1,2,8,4,5,7,6,3), \\ (1,3,9,5,6,8,7,4), \\ (1,4,2,6,7,9,8,5), \\ (1,5,3,7,8,2,9,6), \\ (1,6,4,8,9,3,2,7), \\ (1,7,5,9,2,4,3,8), \\ (1,8,6,2,3,5,4,9), \\ (1,9,7,3,4,6,5,2) \end{array} \right\}$$

$$V_5 = \left\{ \begin{array}{c} (2,6)(3,7)(4,8)(5,9), \\ (1,2)(3,5)(4,7)(8,9), \\ (1,3)(2,9)(4,6)(5,8), \\ (1,4)(2,3)(5,7)(6,9), \\ (1,5)(2,7)(3,4)(6,8), \\ (1,6)(3,8)(4,5)(7,9), \\ (1,7)(2,8)(4,9)(5,6), \\ (1,8)(2,5)(3,9)(6,7), \\ (1,9)(2,4)(3,6)(7,8) \end{array} \right\}, V_6 = \left\{ \begin{array}{c} (2,7,4,9,6,3,8,5), \\ (1,2,5,6,4,3,7,9), \\ (1,3,6,7,5,4,8,2), \\ (1,4,7,8,6,5,9,3), \\ (1,5,8,9,7,6,2,4), \\ (1,6,9,2,8,7,3,5), \\ (1,7,2,3,9,8,4,6), \\ (1,8,3,4,2,9,5,7), \\ (1,9,4,5,3,2,6,8), \end{array} \right\}, V_7 = \left\{ \begin{array}{c} (2,8,6,4)(3,9,7,5), \\ (1,2,7,8)(4,6,9,5), \\ (1,3,8,9)(2,6,5,7), \\ (1,4,9,2)(3,7,6,8), \\ (1,5,2,3)(4,8,7,9), \\ (1,6,3,4)(2,5,9,8), \\ (1,7,4,5)(2,9,3,6), \\ (1,8,5,6)(2,4,7,3), \\ (1,9,6,7)(3,5,8,4), \end{array} \right\}, V_8 = \left\{ \begin{array}{c} (2,9,8,7,6,5,4,3), \\ (1,2,3,6,8,5,9,7), \\ (1,3,4,7,9,6,2,8), \\ (1,4,5,8,2,7,3,9), \\ (1,5,6,9,3,8,4,2), \\ (1,6,7,2,4,9,5,3), \\ (1,7,8,3,5,2,6,4), \\ (1,8,9,4,6,3,7,5), \\ (1,9,2,5,7,4,8,6), \end{array} \right\}$$

Théorème 6. *Deux plans affines standards sont isomorphes si et seulement si leurs pelotes sont isomorphes.*

Démonstration.

$\boxed{\Rightarrow}$ D'après la Proposition 5 on peut toujours se ramener à un isomorphisme de plans standards $f : (\mathbb{A}_d, \mathscr{D}) \longrightarrow (\mathbb{A}_d, \mathscr{D}')$. On note (X_i, Y_j) les coordonnées de $(\mathbb{A}_d, \mathscr{D})$ et (X'_i, Y'_j) celles de $(\mathbb{A}_d, \mathscr{D}')$. On note aussi

D_0 et D'_0 leurs diagonales respectives. Puisque f est un morphisme de plans standards il vérifie $f\left(\overrightarrow{X_1}\right) = \overrightarrow{X'_1}, f\left(\overrightarrow{Y_1}\right) = \overrightarrow{Y'_1}$, et $f(D_0) = D'_0$. On en déduit qu'il existe des permutations σ_X, σ_Y et $\sigma_0 \in \mathfrak{S}_d$ telles que $\forall i, j, f(X_i) = X'_{\sigma_X(i)}, f(X_j) = X'_{\sigma_Y(j)}$ et $f(i,i) = (\sigma_0(i), \sigma_0(i))$ mais pour tout

$$i, j, f(i,j) = f(X_i \cap Y_j) = f(X_i) \cap f(Y_j) = (\sigma_X(i), \sigma_Y(j)).$$

Donc pour tout $i, (\sigma_X(i), \sigma_Y(i)) = (\sigma_0(i), \sigma_0(i))$ donc $\sigma_X = \sigma_Y = \sigma_0$. On en déduit que $f(i,j) = (\sigma_0(i), \sigma_0(j))$. Soit $D \in \mathscr{D}$ et $f(D) = D' \in \mathscr{D}'$ une droite. Par définition, $\sigma_{D'}$ est définie par la relation On a alors

$$\begin{aligned}(i, \sigma_{D'}(i)) &= D' \cap X'_i \\ &= f(D) \cap f(X_{\sigma_0^{-1}(i)}) \\ &= f(D \cap X_{\sigma_0^{-1}(i)}) \\ &= f(\sigma_0^{-1}(i), \sigma_D(\sigma_0^{-1}(i))) \\ &= (i, \sigma_0(\sigma_D(\sigma_0^{-1}(i))))\end{aligned}$$

i.e. $\sigma_{D'} = \sigma_0 \circ \sigma_D \circ \sigma_0^{-1}$.

$\boxed{\Leftarrow}$ Soient $\mathscr{V}_{\mathscr{D}} = [V_1, \ldots, V_{d-1}], \mathscr{V}_{\mathscr{D}'} = \left[V'_1, \ldots, V'_{d-1}\right]$ deux pelotes isomorphes de plans affines standards $(\mathbb{A}_d, \mathscr{D})$ et $(\mathbb{A}_d, \mathscr{D}')$. Soit $\sigma_0 \in \mathfrak{S}_d$ tel que $\mathscr{V}_{\mathscr{D}'} = \sigma_0 \mathscr{V}_{\mathscr{D}} \sigma_0^{-1}$. On pose

$$\begin{array}{rccc} f: & \mathbb{A}_d & \longrightarrow & \mathbb{A}_d \\ & (i,j) & \longrightarrow & (\sigma_0(i), \sigma_0(j)). \end{array}$$

et on vérifie qu'il s'agit d'un isomorphisme de plans standards affines. Pour $D \in \mathscr{D} \setminus \{X_1, \ldots, X_d\} \cup \{Y_1, \ldots, Y_d\}$ on peut écrire $D = D_\sigma$ pour un certain $\sigma \in \mathfrak{S}_d$, i.e. $D = \{(i, \sigma(i)), i \in E_d\}$. Donc $f(D_\sigma) = \{(\sigma_0(i), \sigma_0(\sigma(i))), i \in E_d\}$. Avec le changement de variable $j = \sigma(i)$ on a finalement

$$f(D_\sigma) = \left\{(j, \sigma_0(\sigma(\sigma_0^{-1}(j)))), j \in E_d\right\} = D'_{\sigma_0 \sigma \sigma_0^{-1}}$$

qui est bien une droite de $\mathscr{D}'$ puisque $\sigma \in V_k$ pour un certain k donc $\sigma_0 \sigma \sigma_0^{-1} \in V'_k$. Puisque f est bijectif il s'agit d'un isomorphisme de plans affines d'après la Proposition 3. Finalement, on a $f(X_i) = \left\{(\sigma_0(i), \sigma_0(j)), j \in E_d\right\} = X'_{\sigma_0(i)}$, de même $f(Y_j) = Y_{\sigma_0(j)}$ et $f(i,i) = (\sigma_0(i), \sigma_0(i))$ donc $f(D_0) = D'_0$. Donc f est un morphisme de plans affines standards.

□

Proposition 6. *Soit $\mathscr{V} = [V_1, \ldots, V_{d-1}]$ une pelote, $1 \leq i \leq d-1$ et $\sigma_0 \in V_i$. Alors $\sigma_0^{-1}\mathscr{V} = [\sigma_0^{-1}V_1, \ldots, \sigma_0^{-1}V_{d-1}]$ et $\mathscr{V}\sigma_0^{-1} = [V_1\sigma_0^{-1}, \ldots, V_{d-1}\sigma_0^{-1}]$ sont des pelotes isomorphes à $\mathscr{V}$.*

Démonstration. On montre chacun des axiomes.

- On a $\mathrm{id} \in \sigma_0^{-1}V_i$
- On a toujours $\#\sigma_0^{-1}V_k = d$
- Soit $k \in \{1, \ldots, d-1\}, \sigma_0^{-1}\sigma \neq \sigma_0^{-1}\tau \in \sigma_0^{-1}V_k$ alors on a

$$\mathrm{Supp}\left(\sigma_0^{-1}\sigma\left(\sigma_0^{-1}\tau\right)^{-1}\right) = \mathrm{Supp}\left(\sigma_0^{-1}\sigma\tau^{-1}\sigma_0\right) = \sigma_0\left(\mathrm{Supp}\left(\sigma\tau^{-1}\right)\right)$$

donc on a bien $\#\mathrm{Supp}\left(\sigma_0\sigma\left(\sigma_0^{-1}\tau\right)\right) = \mathrm{Supp}(\sigma\tau^{-1})$.

- Même chose pour $k \neq \ell \in \{1,\dots,d-1\}, \sigma_0^{-1}\sigma \in V_k, \sigma_0^{-1}\tau \in V_\ell$ on a bien

$$\#\mathrm{Supp}\left(\sigma_0\sigma\left(\sigma_0^{-1}\tau\right)^{-1}\right) = d-1.$$

Ce qui prouve que $\sigma_0^{-1}\mathscr{V}$ est une pelote. En fait, en prouvant que $\sigma_0^{-1}\mathscr{V}$ est isomorphe à $\mathscr{V}$ cela prouvera que $\sigma_0^{-1}\mathscr{V}$ est la pelote d'un plan standard donc qu'il s'agit d'une pelote mais j'ai préféré laissé la preuve directe ci-dessus parce que j'avais trop le seum de l'avoir écrite et de l'effacer juste après.

On montre que $\sigma_0^{-1}\mathscr{V}$ et $\mathscr{V}$ sont isomorphes. Soit $(\mathbb{A}_d, \mathscr{D})$ un plan affine standard dont $\mathscr{V}$ est la pelote. On considère $(X_1,\dots,X_d)$ et $(Y_1,\dots,Y_d)$ ses coordonnées et D_0 sa diagonale. Il est clair que le plan $(\mathbb{A}_d, \mathscr{D}')$ ayant pour coordonnées $(X_1,\dots,X_d)$ et $(Y_1',\dots,Y_n') = (Y_{\sigma_0(1)},\dots,Y_{\sigma_0(d)})$ est isomorphes à $(\mathbb{A}_d, \mathscr{D})$ puisqu'ils ont les mêmes droites; on a seulement changer les indices d'une directions. D'autre part la droite $D_{\sigma_0} \in \mathscr{D}$ est définie par $D_{\sigma_0} = \{(i,\sigma_0(i)) \mid i \in E_d\} = \left\{X_i \cap Y_{\sigma_0(i)} \mid i \in E_d\right\} = \left\{X_i \cap Y_i' \mid i \in E_d\right\}$ donc il s'agit de la diagonale de $(\mathbb{A}_d, \mathscr{D}')$. Ce dernier est donc un plan standard. Si on considère une droite $D_\sigma \in \mathscr{D}$ alors ses coordonnées dans $(\mathbb{A}_d, \mathscr{D}')$ sont

$$D_\sigma = \{(i,\sigma(i)) \mid i \in E_d\} = \left\{X_i \cap Y_{\sigma(i)} \mid i \in E_d\right\} = \left\{X_i \cap Y_{\sigma_0(\sigma_0^{-1}\sigma(i))} \mid i \in E_d\right\}$$

Donc dans le système de coordonnées $(X_1,\dots,X_d),(Y_1',\dots,Y_d')$ la droite D_σ a pour permutation $\sigma_0^{-1}\sigma \in \mathfrak{S}_d$.

La preuve que $\mathscr{V}\sigma_0^{-1}$ est une pelote isomorphe à $\mathscr{V}$ est similaire à celle ci-dessus. Il faut seulement permuter les abscisses (X_i) au lieu des ordonnées (Y_j). □

4 Plans affines de Moulton

4.1 Plans de Moulton réel

Je me suis inspiré des plans de Moulton réels qui offrent des exemples de géométries dans lesquels le Théorème de Desargues n'est pas vérifié. Ils sont plus plus intuitifs à appréhender dans $\mathbb{R}^2$ que dans les corps finis comme je le fais dans le paragraphe suivant. Alors, même si ce paragraphe ne sert plus ensuite, je préfère l'écrire tout de même pour faciliter la compréhension de la lectrice.

On considère $A = \mathbb{R}^2$ et on définit les droites affines dites *moultoniennes* comme étant soit les droites verticales usuelles, soit les droites affines de pente positive, soit comme étant les ensembles de la forme

$$D_{[a:\,b:\,c]} = \left\{(x,y) \in \mathbb{R}^- \times \mathbb{R} / ax+by+c=0\right\} \cup \left\{(x,y) \in \mathbb{R}^+ \times \mathbb{R} / 2ax+by+c=0\right\}$$

pour $(a,b,c) \in \mathbb{R}^3 \setminus \{0\}$ lorsque $ab < 0$. Visuellement, la pente de la droite double après avoir passé $x = 0$; le graphe de la droite subit une sorte de diffraction.
En fait, on pourrait remplacer 2 par n'importe quel réel strictement positif (n'importe quel carré non nul de $\mathbb{R}$).

4.2 Plan de Moulton fini

Ma première idée était de calquer l'idée des plans de Moulton réels aux corps finis de cette façon :
Soit $\mathbb{F}_q$ un corps fini et S l'ensemble de ses carrés. On choisit un carré $s \in S$ (l'analogue de 2 pour le cas réel) et on définit les droites comme étant les droites verticales et affines usuelles $D_{a,b} = \left\{y = ax+b\right\}$ lorsque a est un carré (l'analogue de $a \geq 0$ pour le cas réel) et

$$D_{a,b} = \left\{(x, ax+b), x \in \mathbb{F}_q \setminus S\right\} \cup \{(x, sax+b), x \in S\}.$$

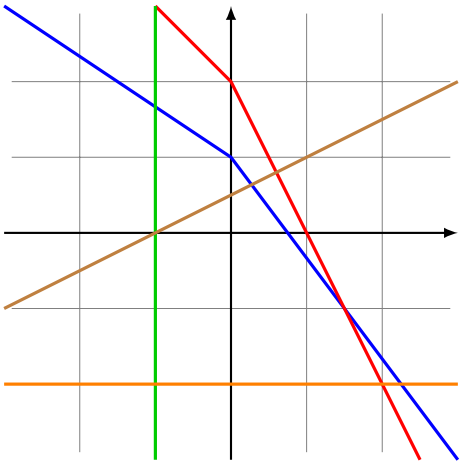


FIGURE 6 – Droites moultoniennes dans un plan de Moulton réel

Malheureusement, je me suis rendu compte que cela donne bien un plan affine dans le cas réel car l'ensemble des carrés réels est stable par addition (la somme de réels positifs est positive) et de même pour les non-carrés de $\mathbb{R}$ mais ça n'est jamais le cas dans les corps finis (car tout élément de $\mathbb{F}_q$ est de la forme x^2+y^2). Je définis donc les plans de Moulton sur $\mathbb{F}_{q^2}$ de façon plus compliquée mais au moins ça donne bien des plans affines qui semblent être non-isomorphes aux plans affines canoniques.

Soit $q=p^e$ une puissance d'un nombre premier p impair. On pose alors $k=\mathbb{F}_q$ et $K=\mathbb{F}_{q^2}$. On note aussi $x\mapsto \overline{x}$ l'unique automorphisme non trivial de $\mathrm{Gal}(K/k)$ et

$$\begin{array}{rccc} N: & K & \longrightarrow & k \\ & x & \longmapsto & x\overline{x} \end{array}$$

l'application norme, qui induit un morphisme de groupe sur les groupes multiplicatifs. On considère l'ensemble $\mathbb{A}_K=K^2$ qui peut être muni d'une structure de plan affine issue de sa structure vectorielle canonique. Dans cette section on souhaite le munir d'une autre structure non-isomorphe à sa structure affine canonique. On notera aussi S_K l'ensemble des carrés de K.

Pour définir une structure de plan affine fini on doit définir les droites $\mathscr{D}_K^{\mathrm{mol}}$ de $\mathbb{A}_K$. On les définit comme étant les ensembles :

- Les droites verticales $\{x=a\}=\{(a,y),y\in K\}$.
- Les ensembles
$$\overline{D}_{a,b}=\{(x,ax+b),x\in K\setminus S\}\cup\{(x,\overline{a}x+b),x\in S\}.$$

On note $\overline{D}_{a,b}$ les droites les deux derniers points et $D_{a,b}=\{(x,ax+b),x\in K\}$ les droites affines du plan affine canonique sur $\mathbb{A}_K$.

Remarque 2. *Lorsque $a\in k$, on a $\overline{a}=a$ et donc il s'agit de la droite affine usuelle $y=ax+b$.*

Théorème 7. *Le couple $(\mathbb{A}_K,\mathscr{D}_K^{mol})$ défini ci-dessus a une structure de plan affine fini.*

Démonstration. On utilise la Proposition 2 car je n'arrive pas à montrer l'axiome 2 de façon directe. Il est clair que toutes les droites ont bien q^2 points. Les droites $x=a_i$ constituent une direction de q^2 droites. Les droites affines $y=ax+b$ constituent pour chaque a dans k une direction différente δ_a et chaque direction est bien constituée de q^2 droites (lorsque b parcourt K). Enfin, soit $a\in K\setminus k$ et $\delta_a=\left\{\overline{D}_{a,b},b\in K\right\}$ qui contient bien q^2 droites. Si $b\neq b'$ on a $\overline{D}_{a,b}\cap\overline{D}_{a,b'}=\emptyset$ (car l'intersection est

vide pour les points d'abscisse parcourant $K \setminus S$ et puis S pour des raisons évidentes). On a donc bien $1+q+q^2-q = q^2+1$ directions.

Il ne reste plus qu'à vérifier que les intersections deux à deux des droites sont de cardinal au plus 1. C'est clair pour les droites verticales et les droites affines usuelles, i.e. $\overline{D}_{a,b}$ pour $a \in k$. Soit $D \in \mathscr{D}_K^{\text{mol}}$, $a' \in K \setminus k$ et $b' \in K$ et $D' = \overline{D}_{a',b'}$.
On distingue les deux cas D verticale et $D = \overline{D}_{a,b}$.

Si D verticale : On pose $D = \{x = a\}$ on a alors $D \cap D' = (a, aa'+b)$ ou alors $D \cap D' = (a, a\overline{a'}+b)$ suivant si $a \in k$ ou $a \in K \setminus k$. Donc une seule intersection.

Si $D = \overline{D}_{a,b}$: Si $a = a'$ alors D et D' ont même direction et sont donc soit parallèles soit confondues. On suppose donc que $a \neq a'$. On considère les systèmes

$$(E_{K\setminus S}) : \begin{cases} y &= ax+b \\ y &= a'x+b' \end{cases} \quad (E_S) : \begin{cases} y &= \overline{a}x+b \\ y &= \overline{a'}x+b' \end{cases}$$

qui auraient pour solution $x_1 = \frac{b'-b}{a-a'}$ et $x_2 = \frac{b'-b}{\overline{a}-\overline{a}'}$ respectivement s'il s'agissait de droites affines. Cependant,

$$\frac{b'-b}{a-a'} = \frac{(b'-b)\left(\overline{a}-\overline{a}'\right)}{(a-a')\left(\overline{a}-\overline{a}'\right)} = \frac{b'-b}{\overline{a}-\overline{a}'} \cdot \frac{N(a-a')}{(a-a')^2}.$$

Puisque, $N(a-a') \in k \subseteq S$ d'après la Proposition 7 et que $(a-a')^2 \in S$ le nombre x_1 diffère de x_2 d'un carré donc est un carré si, et seulement si x_2 en est un. Autrement dit, $(E_{K\setminus S})$ a une solution d'abscisse dans S si et seulement si (E_S) en a aussi une d'abscisse dans S sinon les deux solutions ont leur abscisse dans $K \setminus S$. Donc D croise D' soit sur S soit sur $K \setminus S$.

□

Exemple 9. *Voici la pelote du plan de Molton sur* $\mathbb{F}_9$.

$$V_1 = \left\{ \begin{array}{c} \text{id}, \\ (1,2,6)(3,4,9)(5,8,7), \\ (1,3,7)(2,4,5)(6,9,8), \\ (1,4,8)(2,9,7)(3,5,6), \\ (1,5,9)(2,8,3)(4,6,7), \\ (1,6,2)(3,9,4)(5,7,8), \\ (1,7,3)(2,5,4)(6,8,9), \\ (1,8,4)(2,7,9)(3,6,5), \\ (1,9,5)(2,3,8)(4,7,6), \end{array} \right\}, V_2 = \left\{ \begin{array}{c} (2,6)(3,7)(4,8)(5,9), \\ (1,2)(3,5)(4,7)(8,9), \\ (1,3)(2,9)(4,6)(5,8), \\ (1,4)(2,3)(5,7)(6,9), \\ (1,5)(2,7)(3,4)(6,8), \\ (1,6)(3,8)(4,5)(7,9), \\ (1,7)(2,8)(4,9)(5,6), \\ (1,8)(2,5)(3,9)(6,7), \\ (1,9)(2,4)(3,6)(7,8), \end{array} \right\}, V_3 = \left\{ \begin{array}{c} (2,5,6,9)(3,4,7,8), \\ (1,2,8,4,5)(3,9,6), \\ (1,3,5,9,4)(6,8,7), \\ (1,4,2,6,7)(3,8,5), \\ (1,5,7,3,6)(2,9,8), \\ (1,6,4,8,9)(2,7,5), \\ (1,7,9,5,8)(2,4,3), \\ (1,8,6,2,3)(4,9,7), \\ (1,9,3,7,2)(4,6,5), \end{array} \right\}, V_4 = \left\{ \begin{array}{c} (2,8,6,4)(3,5,7,9), \\ (1,2,7,3,8)(4,6,9), \\ (1,3,2,6,5)(7,8,9), \\ (1,4,9,5,2)(3,6,8), \\ (1,5,4,8,7)(2,3,9), \\ (1,6,3,7,4)(2,5,8), \\ (1,7,6,2,9)(3,4,5), \\ (1,8,5,9,6)(2,4,7), \\ (1,9,8,4,3)(5,6,7), \end{array} \right\},$$

$$V_5 = \left\{ \begin{array}{c} (2,3,6,7)(4,5,8,9), \\ (1,2,4,8,3)(5,7,6), \\ (1,3,9,5,6)(2,7,4), \\ (1,4,6,2,5)(7,9,8), \\ (1,5,3,7,8)(4,9,6), \\ (1,6,8,4,7)(2,9,3), \\ (1,7,5,9,2)(3,8,6), \\ (1,8,2,6,9)(3,5,4), \\ (1,9,7,3,4)(2,8,5), \end{array} \right\}, V_6 = \left\{ \begin{array}{c} (2,9,6,5)(3,8,7,4), \\ (1,2,3,7,9)(5,6,8), \\ (1,3,6,2,8)(4,7,5), \\ (1,4,5,9,3)(2,7,8), \\ (1,5,8,4,2)(6,9,7), \\ (1,6,7,3,5)(2,4,9), \\ (1,7,2,6,4)(3,9,8), \\ (1,8,9,5,7)(3,4,6), \\ (1,9,4,8,6)(2,5,3), \end{array} \right\}, V_7 = \left\{ \begin{array}{c} (2,4,6,8)(3,9,7,5), \\ (1,2,9,5,4)(6,7,8), \\ (1,3,8,4,9)(2,5,7), \\ (1,4,3,7,6)(2,8,9), \\ (1,5,2,6,3)(4,7,9), \\ (1,6,5,9,8)(2,3,4), \\ (1,7,4,8,5)(3,6,9), \\ (1,8,7,3,2)(4,5,6), \\ (1,9,6,2,7)(3,5,8), \end{array} \right\}, V_8 = \left\{ \begin{array}{c} (2,7,6,3)(4,9,8,5), \\ (1,2,5,9,7)(3,6,4), \\ (1,3,4,8,2)(6,7,9), \\ (1,4,7,3,9)(5,8,6), \\ (1,5,6,2,4)(3,8,9), \\ (1,6,9,5,3)(2,8,7), \\ (1,7,8,4,6)(2,3,5), \\ (1,8,3,7,5)(2,9,4), \\ (1,9,2,6,8)(4,5,7), \end{array} \right\}$$

Ceci prouve avec le Théorème 6 que le plan affine $(\mathbb{F}_9)^2$ *et le plan de Molton sur* $\mathbb{F}_9$ *ne sont pas isomorphes.*

5 Pelotes des plans affines canoniques et des plans de Molton

5.1 Pelotes des plans affines canoniques

On fixe $q = p^e$ une puissance d'un nombre premier et $\mathbb{A}_q = \mathbb{F}_q^2$ le plan affine canonique muni de sa structure canonique. Étant donnée une droite oblique (ni horizontale ni verticale) $D : y = ax+b \subseteq \mathbb{A}_q$

on considérera $\sigma_D \in \mathfrak{S}(\mathbb{F}_q)$ définie par $\sigma_D(x) = ax + b$ comme définie dans la section 3.2. On considère sa pelote $\mathscr{V}_q = [V_a]_{a\in\mathbb{F}_q^\times}$ où V_a désigne l'ensemble des σ_D pour D de pente a. Cela reste cohérent avec les notations précédentes; V_1 est toujours bien composée des permutations correspondant à la direction diagonale. On commettra parfois l'abus de confondre $\mathscr{V}_q$ avec l'ensemble des éléments des V_a, i.e. $\bigcup_{a\in\mathbb{F}_q^\times} V_a$.

Théorème 8. *Soit $\mathbb{F}_q$ un corps fini, $\mathbb{A}_q = \mathbb{F}_q^2$ le plan affine canonique et $\mathscr{V}_q = \bigcup_{a\in\mathbb{F}_q^\times} V_a$ la pelote correspondante. Alors*

1. *$\mathscr{V}_q$ est un sous-groupe d'ordre $q(q-1)$ de $\mathfrak{S}(\mathbb{F}_q)$.*
2. *L'ensemble V_1 est un sous-groupe distingué de $\mathscr{V}_q$. Il est isomorphe à $\mathbb{F}_q \simeq \mathbb{F}_p^e$, i.e. tous ses éléments non neutres sont produits de e cycles disjoints de taille p.*
3. *Pour tout $a \in \mathbb{F}_q^\times$ les éléments de V_a sont conjugués deux à deux, i.e. ils ont la même décomposition en cycles disjoints.*
4. *On a un isomorphisme de groupes*
$$\mathscr{V}_q \simeq \mathbb{F}_q \rtimes \mathbb{F}_q^\times.$$

Démonstration.

1. Étant donnée une droite oblique D: $y = ax + b$, i.e. $a \neq 0$, on note $\sigma_D = \sigma_{a,b}$ la permutation correspondante définie par $\sigma_{a,b}(x) = ax + b$. On peut alors réécrire $\mathscr{V}_q = \left\{\sigma_{a,b}, a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q\right\}$. On a donc $\sigma_0^1 = \mathrm{id} \in \mathscr{V}_q$. De plus pour $a, c \in \mathbb{F}_q^\times, b, d \in \mathbb{F}_q, \sigma_{a^{-1},-b} \in \mathscr{V}_q$, inverse de σ_b^a et
$$(\sigma_{a,b}\sigma_{c,d})(x) = \sigma_{a,b}(cx + d) = acx + ad + b = \sigma_{ac,ad+b}(x). \tag{1}$$
Donc $\sigma_{a,b}\sigma_{c,d} = \sigma_{ac,ad+b}$ qui est bien un élément de $\mathscr{V}_q$ ce qui prouve le premier point.
2. D'après la relation (1) il est clair que V_1 est un sous-groupe de $\mathscr{V}_q$. Par simplicité on notera σ_b au lieu de $\sigma_{1,b}$ les éléments de V_1. Soit $\sigma_{\alpha,\beta} \in \mathscr{V}_q$ et $\sigma = \sigma_b \in V_1$. On a
$$\left(\sigma_{\alpha,\beta}^{-1}\sigma\sigma_{\alpha,\beta}\right)(x) = \sigma_{\alpha^{-1},-\beta}(\alpha x + \beta + b) = x + \alpha^{-1}\beta + \alpha^{-1}b - \beta.$$
Donc $\sigma_{\alpha,\beta}^{-1}\sigma\sigma_{\alpha,\beta} = \sigma_{\alpha^{-1}\beta+\alpha^{-1}b-\beta} \in V_1$. Donc V_1 distingué dans $\mathscr{V}_q$. D'autre part, étant donné $\sigma_b \in V_1$ avec $b \neq 0$ on a $\sigma_b^k = \sigma_{kb}$ d'après la relation (1). Puisque $\mathbb{F}_q$ est de caractéristique $p, \sigma_p^k = \mathrm{id}$ si et seulement si $p|k$. On en déduit que σ_b est un produit de cycles support disjoint donc les cycles sont de taille 1 ou p mais puisque $\mathrm{Supp}(\sigma_b) = \mathbb{F}_q, \sigma_b$ n'admet pas de cycles de taille 1 (i.e. pas de point fixe). Il s'agit donc d'un produit de e cycles de taille p.
3. Il s'agit la même preuve qu'au dessus; pour $a, \alpha \in \mathbb{F}_q^\times, b, \beta \in \mathbb{F}_q$ on a
$$\sigma_{\alpha,\beta}^{-1}\sigma_{a,b}\sigma_{\alpha,\beta} = \sigma_{a,\alpha^{-1}a\beta+\alpha^{-1}b-\beta}.$$
donc V_a stable par conjugaison par des éléments de $\mathscr{V}_q$.
4. On pose $H = V_1$. L'ensemble $K = \left\{\sigma_{a,0}, a \in \mathbb{F}_q^\times\right\} \simeq \mathbb{F}_q^\times$ est un sous-groupe de $\mathscr{V}_q$ et on a $\mathscr{V}_q = HK$ et $H \cap K = \{\mathrm{id}\}$. Donc $\mathscr{V}_q$ est bien le produit semi-direct de H et de K.

□

Remarque 3.

1. *En reprenant les notations de la démonstration du Théorème 8 on peut expliciter l'isomorphisme* $\mathscr{V}_q \simeq \mathbb{F}_q \rtimes \mathbb{F}_q^\times$ *qui est simplement*

$$\begin{aligned} \mathscr{V}_q &\longrightarrow \mathbb{F}_q \rtimes \mathbb{F}_q^\times \\ \sigma_{a,b} &\longmapsto (b,a) \end{aligned}$$

avec la loi de composition de $\mathbb{F}_q \rtimes \mathbb{F}_q^\times$ *donnée par*

$$(b,a)(d,c) = (ad+b, ac).$$

2. *Soit* $a \in \mathbb{F}_q^\times$. *On montre facilement par récurrence que dans* $\mathbb{F}_q \rtimes \mathbb{F}_q^\times$ *on a* $(b,a)^k = \left(\left(\sum_{j=0}^{k-1} a^j\right) b, a^k\right)$. *Puisque* $\sum_{j=0}^{k-1} a^j = \frac{a^k-1}{a-1}$ *on a* $(b,a)^k = (0,1)$ *si, et seulement si* $a^k = 1$. *Si on note* m *l'ordre de* a *puisque pour tout* $1 \leq j \leq m-1$ *on a* $a^j \neq 1$ *alors* $\sigma_{a,b}^j \in V_{a^j} \neq V_1$ *donc* $\#\mathrm{Supp}(\sigma_{a,b}^j) = q-1$. *On en déduit que* $\sigma_{a,b}$ *est un produit de* $\frac{q-1}{m}$ *cycles disjoints de taille* m.

5.2 Pelotes des plans affines de Molton

On considère $k = \mathbb{F}_q \subseteq K = \mathbb{F}_{q^2}$ et on note γ la conjugaison de K sur k, i.e. $\gamma(x) = x^q$. On note toujours $S_K \subseteq K$ l'ensemble des carrés. On pose aussi δ le logarithme du morphisme de Legendre, i.e. $\delta(x) = \frac{1+\left(\frac{x}{q^2}\right)}{2} \in \{0,1\}$ vu comme un élément de $\mathbb{F}_2$. On a alors un morphisme de groupes

$$\begin{aligned} \delta\colon \quad \mathbb{F}_{q^2}^\times &\longrightarrow \mathbb{F}_2 \\ x &\longmapsto \delta(x) \end{aligned}$$

ceci nous permet de réécrire plus simplement la définition des droites moultoniennes. Si $D\colon\ y = ax+b$ est une droite moultonienne et σ_D est sa permutation associée alors

$$\sigma_D(x) = \gamma^{1+\delta(x)}(a)x + b$$

ce qui nous épargne de distinguer les cas $x \in S$ et $x \notin S$.

Théorème 9. *Le plan affine de Molton sur* $K = \mathbb{F}_{q^2}$ *n'est pas isomorphe au plan affine canonique* $\mathbb{A}_{q^2}$.

Démonstration. On note $\mathscr{V}_{\mathrm{can}}$ la pelote du plan affine canonique $\mathbb{A}_{q^2}$. Pour prouver le théorème il suffit de montrer que la pelote $\mathscr{V}_{\mathrm{mol}} = [V_a]_{a\in K^\times}$ où $V_a = \left\{\sigma\colon x \mapsto \gamma^{1+\delta(x)}(a)x + b\right\} \subseteq \mathfrak{S}(K)$ n'est pas un sous-groupe de $\mathfrak{S}(K)$. En effet, si ces plans étaient isomorphes alors leurs pelotes seraient conjuguées d'après le Théorème 6 or d'après le Théorème 8 $\mathscr{V}_{\mathrm{can}}$ est un sous-groupe de $\mathfrak{S}(K)$ et les conjugués de sous-groupes restent des sous-groupes.

L'idée de la preuve ci-dessous est de trouver deux permutations σ et τ dans la pelote $\mathscr{V}_{\mathrm{mol}}$ telles que $\sigma \circ \tau \notin \mathscr{V}_{\mathrm{mol}}$. Pour cela on va utiliser l'heuristique suivante : les permutations $\sigma(x) = \gamma^{1+\delta(x)}(a) + b$ de la pelote correspondent à des applications affines par morceaux avec au plus deux morceaux sur lesquels elle est affine (lorsque $a \in k$ l'application est affine et lorsque $a \notin k$ elle est affine sur S_K et sur $S_K^c = K \setminus S_K$ respectivement). On va s'arranger pour trouver σ et τ telles que $\sigma\circ\tau$ soit affine par morceaux strictement sur S_K ce qui prouvera que $\sigma \circ \tau \notin \mathscr{V}_{\mathrm{mol}}$.

Pour cela choisissons $a \in K \setminus S_K$ et prenons $\beta \in K \setminus S_K$. On peut toujours écrire $\beta = y^2 + a'^2$ pour un certain $x, a' \in S_K$ d'après la Proposition 8. Quitte à multiplier β par un carré on peut supposer qu'on a $\beta = y^2 + 1$.

Maintenant considérons les permutations $\sigma(x) = \gamma^{1+\delta(x)}(a^{-1})x$ et $\tau(x) = \gamma^{1+\delta(x)}(a)x + a$, i.e. les permutations issues des droites moultoniennes $y = a^{-1}x$ et $y = ax+a$. Alors la permutations $\sigma\circ\tau$ est donnée par $\sigma\circ\tau(x) = \begin{cases} x+1 & \text{pour } x \in \tau^{-1}\left(S_K^c\right) \cap S_K^c \\ x+\gamma(a)^{-1}a & \text{pour } x \in \tau^{-1}(S_K) \cap S_K \\ a^{-1}\gamma(a)x+1 & \text{pour } x \in \tau^{-1}\left(S_K^c\right) \cap S_K \\ \gamma(a)^{-1}a(x+1) & \text{pour } x \in \tau^{-1}(S_K) \cap S_K^c \end{cases}$

Si $\sigma\circ\tau \in \mathscr{V}_{\text{mol}}$ alors il existe $c, d \in K$ tels que pour tout $x \in S_K^c$ on ait $\sigma\circ\tau(x) = \gamma^{1+\delta(x)}(c)x + d$ et pour tout $x \in S_K, \sigma\circ\tau(x) = \gamma(c)x + d$. Maintenant puisqu'il existe y tel que $y^2 + a^2 = \beta$ alors $a^{-1}(y^2+1) = \tau(y^2) = a^{-1}\beta$ qui est un carré car produit de deux non carrés. De même $\tau(\gamma(y)^2) = a^{-1}(\gamma(y)^2 + \gamma(1)) = a^{-1}(\gamma(y)^2+1) = a^{-1}\gamma(\beta)$. De plus $a^{-1}\gamma(\beta)$ est aussi un carré car γ préserve les carrés et les non carrés et il est distinct de $a^{-1}\beta$ car $\beta \notin k$. On en déduit que $\left\{a^{-1}\beta, a^{-1}\gamma(\beta)\right\} \subseteq \tau^{-1}(S_K) \cap S_K$. Cet ensemble est donc de cardinal au moins 2.

Par ailleurs $\tau(k) = a^{-1}k$, un ensemble constitué de q non carrés tous distincts. On a donc $k \subseteq \tau^{-1}(S_K^c) \cap S_K$ qui est donc aussi de cardinal au moins 2. On en déduit d'une part que les écritures $\sigma\circ\tau(x) = \gamma(c)x+d$ et $\sigma\circ\tau(x) = x + \gamma(a)^{-1}a$ coïncident pour au moins deux éléments distincts $x \in S_K$ donc $c = 1$ et $d = \gamma(a)^{-1}a$. De même pour les écritures $\gamma(c)x + d$ et $a^{-1}\gamma(a)x + 1$ ce qui implique que $\gamma(c) = a^{-1}\gamma(a)$ et $d = 1$. Ces conditions imposent que $a = \gamma(a)$, i.e. $a \in k$ ce qui est absurde par l'hypothèse $a \notin S_K$. □

Théorème 10. *Pour toute puissance impaire d'un nombre premier q il existe au moins deux plans projectifs d'ordre q^2 non isomorphes.*

Démonstration. Soit $K = \mathbb{F}_{q^2}$ et $k = \mathbb{F}_q$. On considère $P_{\text{can}} = \mathbb{P}^2(K)$ le projectivisé du plan affine canonique $\mathbb{A}_{q^2}$ et P_{mol} le projectivisé du plan affine de Molton d'ordre q^2. Bien qu'un même plan projectif puisse contenir des plans affines non isomorphes, il est connu que tous les plans affines d'ordre q^2 contenus $\mathbb{P}^2(K)$ sont isomorphes à $\mathbb{A}_{q^2}$. Par conséquent P_{mol} et P_{can} ne peuvent être isomorphes. □

A Rappels sur les corps finis

Soit $\mathbb{F}_q$ un corps fini à $q = p^s$ éléments avec p impair. On rappelle que $\mathbb{F}_q$ est l'unique corps fini à q élément à isomorphisme près. De plus il existe un morphisme de groupes

$$\begin{aligned}\left(\frac{\cdot}{q}\right): \quad \mathbb{F}_q^\times &\longrightarrow \{-1,1\} \\ x &\longmapsto x^{\frac{q-1}{2}}\end{aligned}$$

tel que $\left(\frac{x}{q}\right) = 1$ si, et seulement si x est un carré dans $\mathbb{F}_q$.

Proposition 7. *On considère l'extension de corps $\mathbb{F}_q \to \mathbb{F}_{q^2}$. Alors tout élément de $\mathbb{F}_q$ est un carré dans $\mathbb{F}_{q^2}$.*

Démonstration. Je propose deux jolies preuves de ce résultat.

Première méthode : Soit $a \in \mathbb{F}_q$. Si a est un carré dans $\mathbb{F}_q$ alors c'est aussi évidemment un carré dans $\mathbb{F}_{q^2}$ sinon le polynôme $X^2 - a \in \mathbb{F}_q[X]$ est irréductible et donc $K = \mathbb{F}_q[X]/\langle X^2 - a\rangle$ est une extension de $\mathbb{F}_q$ de degré 2 donc de cardinal q^2. On en déduit par unicité que $K \simeq \mathbb{F}_{q^2}$ donc a est un carré dans $\mathbb{F}_{q^2}$ (l'image de la classe de X par l'isomorphisme).

Deuxième méthode : Soit $a \in \mathbb{F}_q^\times$. On a $a^{\frac{q^2-1}{2}} = \left(a^{\frac{q-1}{2}}\right)^{q+1}$ mais $a^{\frac{q-1}{2}} \in \{-1,1\}$ et $q+1$ pair donc $a^{\frac{q^2-1}{2}} = 1$ donc a est un carré dans $\mathbb{F}_{q^2}$.

□

On pourrait de la même façon prouver plus généralement que $a \in \mathbb{F}_q$ est un carré dans $\mathbb{F}_{q^n}$ si et seulement si n est pair ou a est un carré dans $\mathbb{F}_q$.

Proposition 8. *Soit K un corps fini. Alors tout élément de K est somme de deux carrés.*

Démonstration. Si K est de caractéristique 2 c'est évident puisque tout élément de K est un carré.

Sinon supposons que K ait q éléments. Soit a un élément quelconque de K. On sait que K admet $\frac{q+1}{2}$ carrés au total (0 inclus). On note S_K l'ensemble de ses carrés. On considère l'application

$$\begin{aligned}\varphi: \quad S_K &\longrightarrow K \\ s &\longmapsto a - s.\end{aligned}$$

Il s'agit d'une application injective donc son image est de cardinal $\frac{q+1}{2}$ donc elle rencontre S_K autrement on aurait $\#K \geq 2\frac{q+1}{2} = q+1$ ce qui est absurde. Si $t \in S_K \cap \operatorname{im}\varphi$ on a $x = s + t$ donc x est bien somme de deux carrés. □

B Résultats archivés

Dans cette section je place quelques résultats qui m'avaient semblé utiles mais que je n'ai finalement pas utilisé.

B.1 Quelques résultats sur les permutations

Soit d un entier et $\mathfrak{S}_d$ le groupe des permutations de $E_d = \{1,\dots,d\}$. On rappelle qu'il existe un morphisme $\varepsilon\colon \mathfrak{S}_d \longrightarrow \{-1,1\}$ qui vérifie $\forall i \neq j, \varepsilon((i\,j)) = -1$. Le nombre $\varepsilon(\sigma)$ est appelé la *signature* de σ.

Lemme 1. *Soient $\sigma,\tau \in \mathfrak{S}_d$ alors*

$$\mathrm{Supp}(\sigma^{-1}\tau\sigma) = \sigma\big(\mathrm{Supp}(\tau)\big).$$

Démonstration. On a

$$i \notin \mathrm{Supp}(\sigma^{-1}\tau\sigma) \Leftrightarrow \sigma^{-1}\tau\sigma(i) = i \Leftrightarrow \tau(\sigma(i)) = \sigma(i) \Leftrightarrow \sigma(i) \notin \sigma\big(\mathrm{Supp}(\tau)\big).$$

□

Lemme 2. *Soit $\sigma \in \mathfrak{S}_d$ une permutation. On suppose que la décomposition de σ en cycle à support disjoint est $\sigma = c_1 c_2 \cdots c_{\ell_1} c_{\ell_1+1} \cdots c_{\ell_2} \cdot c_{\ell_{r-1}+1} \cdots c_{\ell_r}$ avec $\forall i, c_{\ell_{i-1}+1},\dots,c_{\ell_i}$ cycle de taille d_i et $d_1 < \cdots < d_r$. Alors la classe de conjugaison Ω_σ de σ est de cardinal*

$$\#\Omega_\sigma = \frac{d!}{(d-(\ell_1 d_1 + \cdots + \ell_r d_r))! d_1^{\ell_1}\ell_1! \cdots d_r^{\ell_r}\ell_r!}.$$

Démonstration. On considère un cycle $c = (a_1\ a_2\ \dots\ a_n)$ alors $\forall \tau \in \mathfrak{S}_d$ on a $\tau c \tau^{-1} = (\tau(a_1)\,\tau(a_2)\ \dots\ \tau(a_n))$. On a alors d choix pour $\tau(a_1)$ puis $d-1$ pour $\tau(a_2)$ puis, par récurrence, $d-n+1$ pour $\tau(a_n)$. Puisqu'une permutation cyclique des $\tau(a_i)$ donne le même cycle la classe de conjugaison de c est de cardinal $\frac{d!}{(d-n)!n}$. On a donc $\frac{d!}{(d-d_1)!d_1}$ choix pour le cycle c_1 puis, en considérant $\tau c_2 \cdots c_{\ell_r}\tau^{-1}$ comme une permutation de $\{1,\dots,d\} \setminus \{\tau(a_i), i \in 1,\dots,d_1\}$ on a $\frac{(d-d_1)!}{(d-d_1-d_1)!d_1}$ choix si c_2 de taille d_1 et $\frac{(d-d_1)!}{(d-d_1-d_2)!d_2}$ sinon. En procédant par récurrence on a donc

$$\frac{d!}{(d-d_1)!d_1} \cdot \frac{(d-d_1)!}{(d-2d_1)!d_1} \cdots \frac{(d-(\ell_1-1)d_1)!}{(d-\ell_1 d_1)!d_1} \cdots \frac{(d-(\ell_1 d_1 + \cdots + (\ell_r-1)d_r))!}{(d-(\ell_1 d_1 + \cdots + \ell_r d_r))!d_r}.$$

Ce qui vaut $\frac{d!}{(d-(\ell_1 d_1+\cdots+\ell_r d_r))! d_1^{\ell_1}\cdots d_r^{\ell_r}}$ par télescopage. Enfin, on remarque que chaque cycle de même longueur d_i a été compté plusieurs fois car l'ordre n'importe pas. On a $\ell_i!$ façon de les réordonner ce qui donne

$$\#\Omega_\sigma = \frac{d!}{(d-(\ell_1 d_1 + \cdots + \ell_r d_r))! d_1^{\ell_1}\ell_1! \cdots d_r^{\ell_r}\ell_r!}.$$

□

Exemple 10. *On considère $\sigma = (1,2)(3,4)(5,6) \in \mathfrak{S}_6$. On a $r = 1, d_1 = 2$ et $\ell_1 = 3$ ce qui donne $\#\Omega_\sigma = \frac{6!}{0!2^3\cdot 3!} = 15$. En effet, on peut vérifier que*

$$\begin{aligned}\Omega_\sigma = \{&(1,2)(3,5)(4,6),(1,3)(2,5)(4,6),(1,5)(2,3)(4,6),(1,6)(2,4)(3,5),(1,3)(2,4)(5,6),\\ &(1,4)(2,6)(3,5),(1,4)(2,3)(5,6),(1,2)(3,4)(5,6),(1,4)(2,5)(3,6),(1,2)(3,6)(4,5),\\ &(1,5)(2,4)(3,6),(1,6)(2,5)(3,4),(1,3)(2,6)(4,5),(1,6)(2,3)(4,5),(1,5)(2,6)(3,4)\}\end{aligned}$$

Proposition 9. *Soit $\sigma,\tau \in \mathfrak{S}_d$ tel qu'il existe $g \in \mathfrak{S}_d$ tel que $g^{-1}\sigma g = \tau$ alors*

$$\big\{h \in \mathfrak{S}_d \mid h^{-1}\sigma h = \tau\big\} = C(\sigma)g$$

où $C(\sigma)$ est le centralisateur de σ, i.e. l'ensemble des éléments de $\mathfrak{S}_d$ qui commutent avec σ.

Démonstration. Soit h tel que $h^{-1}\sigma h = \tau$ alors $h^{-1}\sigma h = g^{-1}\sigma g$, i.e. $\sigma h g^{-1} = h g^{-1}\sigma$ donc on a bien $hg^{-1} \in C(\sigma)$. Réciproquement, si $\gamma \in C(\sigma)$ et $h = \gamma g$ alors $h^{-1}\sigma h = g^{-1}\gamma^{-1}\sigma\gamma\sigma = g^{-1}\sigma g = \tau$. □

B.2 Une structure de groupe exotique

Au départ je voulais utiliser cette section pour prouver que les plans de Moulton ne sont jamais isomorphes à des plans affines en prouvant que le groupe $\mathbb{F}_q^2 \rtimes (\mathbb{F}_q^2)^\times$ ne possède pas de sous-groupe isomorphe au groupe $(\mathbb{F}_q^2, \star)$ que l'on va définir. Finalement je suis parti dans une autre direction mais je garde ces résultats sous la main parce que c'est amusant.

B.2.1 Définitions

Dans la Section 5.2 on a prouvé que la pelote du plan de Molton sur $K = \mathbb{F}_{q^2}$ n'étaient jamais un sous-groupes de $\mathfrak{S}(K)$. Je me suis demandé s'il contenait tout de même des sous-groupes, en particulier j'avais l'impression qu'en considérant uniquement les $\sigma(x) = \gamma^{1+\delta(x)}(a)x$ (correspondant aux droites moultoniennes sans « ordonnée à l'origine ») ça donnerait un sous-groupe de $\mathfrak{S}(K)$ qu'on peut identifié à $K^\times$ en considérant seulement la pente a. J'étais très étonné qu'on puisse munir $K^\times$ d'une structure de groupe aussi algébrique (qui exploite non seulement le caractère δ mais aussi le Frobenius γ) alors je mets quelques résultats relatifs à ce groupe dans les sections suivantes.

On définit une loi de composition interne sur $K^\times$

$$\forall a, b \in K^\times, a \star b = \gamma^{\delta(b)}(a)b$$

Lemme 3. *Le magma $(K^\times, \star)$ est un groupe.*

Démonstration. Il faut montrer que la loi est associative, qu'il existe un élément neutre et un inverse pour tout élément de $K^\times$.

$\star$ est associative : Soient $a, b, c \in K^\times$. Alors

$$\begin{aligned}(a \star b) \star c &= (\gamma^{\delta(b)}(a)b) \star c \\ &= \gamma^{\delta(c)}(\gamma^{\delta(b)}(a)b)c \\ &= \gamma^{\delta(c)+\delta(b)}(a)\gamma^{\delta(c)}(b)c \\ &= \gamma^{\delta(bc)}(a)\gamma^{\delta(c)}(b)c\end{aligned}$$

et d'autre part

$$\begin{aligned}a \star (b \star c) &= \gamma^{\delta(b\star c)}(a)(b \star c) \\ &= \gamma^{\delta(\gamma^{\delta(c)}(b)c)}(a)\gamma^{\delta(c)}(b)c \\ &= \gamma^{\delta(\gamma^{\delta(c)}(b)+\delta(c)}(a)\gamma^{\delta(c)}(b)c \\ &= \gamma^{\delta(b)+\delta(c)}(a)\gamma^{\delta(c)}(b)c && \text{car } b \in S \Leftrightarrow \gamma(b) \in S \\ &= (a \star b) \star c.\end{aligned}$$

$\star$ possède un élément neutre : En effet on a pour tout $a \in K^\times$,

$$a \star 1 = \gamma^{\delta(1)}(a)1 = \mathrm{id}_K(a) = a \text{ et } 1 \star a = \gamma^{\delta(a)}(1)a = 1 \times a = a.$$

Tout le monde possède un inverse pour $\star$: On montre que pour tout a l'élément $b = \gamma^{\delta(a)}(a^{-1})$ est l'inverse de a pour $\star$. On a

$$\begin{aligned}a \star \gamma^{\delta(a)}(a^{-1}) &= \gamma^{\delta\left(\gamma^{\delta(a)}(a^{-1})\right)}(a)\gamma^{\delta(a)}(a^{-1}) \\ &= \gamma^{\delta(a^{-1})}(a)\gamma^{\delta(a)}(a^{-1}) && \text{car } a^{-1} \in S \Leftrightarrow \gamma(a^{-1}) \in S \\ &= \gamma^{\delta(a)}(a)\gamma^{\delta(a)}(a^{-1}) && \text{car } a \in S \Leftrightarrow a^{-1} \in S \\ &= \gamma^{\delta(a)}(aa^{-1}) = 1\end{aligned}$$

□

De la même façon que dans le cas des plans affines canoniques on note $\sigma_{a,b} \in \mathfrak{S}(K)$ la permutation associée à la droite moultonienne $D\colon\ y = ax + b$ et σ_a celle associée à $y = ax$. De même on note $\widetilde{\mathscr{V}_{q^2}} = \left[\widetilde{V}_1, \ldots, \widetilde{V}_{q^2-1}\right]$ la pelote du plan affine K^2 muni de sa structure moultonienne. On identifie $\widetilde{\mathscr{V}_q}$ avec les éléments des $\widetilde{V}_i$, i.e.

$$\widetilde{\mathscr{V}_{q^2}} = \bigcup_{a\in K^\times, b\in K} \sigma_{a,b}.$$

Proposition 10. *L'ensemble $F = \left\{\sigma_a \mid a \in K^\times\right\}$ est un sous-groupe de $\mathfrak{S}(K)$ isomorphe à $(K^\times, \star)$.*

Démonstration. Soient $a, b \in K^\times$ et $x \in K$. Alors on a

$$\begin{aligned}
(\sigma_a\sigma_b)(x) &= \sigma_a\left(\gamma^{1+\delta(x)}(b)x\right)\\
&= \gamma^{1+\delta\left(\gamma^{1+\delta(x)}(b)x\right)}(a)\gamma^{1+\delta(x)}(b)x\\
&= \gamma^{1+\delta\left(\gamma^{1+\delta(x)}(b)\right)+\delta(b)}(a)\gamma^{1+\delta(x)}(b)x\\
&= \gamma^{1+\delta(b)+\delta(x)}(a)\gamma^{1+\delta(x)}(b)x\\
&= \gamma^{1+\delta(x)}(\gamma^{\delta(b)}(a))\gamma^{1+\delta(x)}(b)x\\
&= \gamma^{1+\delta(x)}(\gamma^{\delta(b)}(a)b)x\\
&= \sigma_{\gamma^{\delta(b)}(a)b}(x).
\end{aligned}$$

Ceci prouve que F est un sous-groupe de $\mathfrak{S}(K)$ et l'application

$$\begin{aligned}
(K^\times, \star) &\longrightarrow F\\
a &\longmapsto \sigma_a
\end{aligned}$$

est un isomorphisme de groupes.

□

B.2.2 Étude du groupe $(K^\times, \star)$

On souhaite déterminer la structure de $(K^\times, \star)$.

Lemme 4. *Soit $a \in K^\times$ alors les puissances de a sont données par*

$$\begin{cases} a^{\star 2n} &= \gamma^{\delta(a)}(a)^n a^n\\ a^{\star 2n+1} &= \gamma^{\delta(a)}(a)^n a^{n+1}\end{cases}$$

Démonstration. On fait une récurrence sur n. Au rang $n = 0$ on a bien $a^{\star 0} = 1$ d'une part et $\gamma^{\delta(a)}(a)^0 a^0 = 1$ d'autre part et $a^{\star 1} = a = \gamma^{\delta(a)}(a)^0 a$. Soit $n \geq 0$ tel qu'on ait

$$\begin{cases} a^{\star 2n} &= \gamma^{\delta(a)}(a)^n a^n\\ a^{\star 2n+1} &= \gamma^{\delta(a)}(a)^n a^{n+1}\end{cases}$$

On veut montrer ces deux relations au rang $n+1$. On a

$$a^{\star 2n+2} = a^{\star 2n+1} \star a = \gamma^{\delta(a)}\left(\gamma^{\delta(a)}(a)^n a^{n+1}\right)a = a^n\gamma^{\delta(a)}(a)^{n+1}a = \gamma^{\delta(a)}(a)^{n+1}a^{n+1}$$

et

$$a^{\star 2n+3} = a^{\star 2n+2}a = \gamma^{\delta(a)}\left(\gamma^{\delta(a)}(a)^{n+1}a^{n+1}\right)a = \gamma^{\delta(a)}(a)^{n+1}a^{n+2}.$$

□

Lemme 5. *On a les deux proposition suivantes*

1. *L'ensemble $S^\times$ des carrés de $K^\times$ est un sous-groupe distingué commutatif de $(K^\times, \star)$.*
2. *Le centre de $(K^\times, \star)$ est $Z(K^\times) = k^\times$.*

Démonstration. 1. Pour $a, b \in S^\times$ on a $a \star b = \gamma^{\delta(b)}(a)b = ab$ donc il s'agit bien d'un sous-groupe commutatif.
Soit $a \in S^\times, b \in K^\times$ on a

$$\begin{aligned} b^{\star -1} \star a \star b &= \gamma^{\delta(b)}(b^{-1}) \star \gamma^{\delta(b)}(a)b \\ &= \gamma^{\delta(\gamma^{\delta(b)}(a)b)}(\gamma^{\delta(b)}(b^{-1}))\gamma^{\delta(b)}(a)b \\ &= \gamma^{\delta(a)+\delta(b)}(\gamma^{\delta(b)}(b^{-1}))\gamma^{\delta(b)}(a)b \\ &= \gamma^{\delta(b)}(\gamma^{\delta(b)}(b^{-1}))\gamma^{\delta(b)}(a)b \\ &= b^{-1}\gamma^{\delta(b)}(a)b \\ &= \gamma^{\delta(b)}(a) \end{aligned}$$

qui est un carré car a en est un.

2. Soit $a \in k^\times$ alors on rappelle (Proposition 7) que a est un carré dans $K^\times$. On a donc pour tout $b \in K^\times, a \star b = \gamma^{\delta(b)}(a)b = ab$ et $b \star a = \gamma^{\delta(a)}(b)a = ba$.
Réciproquement soit $a \in Z(K^\times)$. Alors pour tout $b \in K^\times$ on a $a \star b = b \star a$, i.e.

$$\gamma^{\delta(b)}(a)b = \gamma^{\delta(a)}(b)a$$

donc pour $b \in S^\times$ on a $ab = \gamma^{\delta(a)}(b)a$, i.e. $b = \gamma^{\delta(a)}(b)$. Puisque $S^\times \setminus k^\times \neq \emptyset$ on a forcément $a \in S^\times$. On en déduit que pour tout $b \in K^\times, \gamma^{\delta(b)}(a)b = ab$ donc $\gamma^{\delta(b)}(a) = a$ donc en prenant $b \in K^\times \setminus k^\times$ on a $a \in k^\times$.

□

Exemple 11. *Le groupe $(\mathbb{F}_9^\times, \star)$ est un groupe non commutatif à 8 éléments. D'après la classification des groupes finis il est donc isomorphe à*

$$D_4 = \left\{\mathrm{id}, \tau, \tau^2, \tau^3, \sigma, \sigma\tau, \sigma\tau^2, \sigma\tau^3\right\},$$

le groupe diédral des isométries du carrés avec τ la rotation d'angle $\frac{\pi}{2}$ et σ une symétrie ou alors $(\mathbb{F}_9^\times, \star)$ est isomorphe à

$$Q_8 = \left\{1, -1, i, j, k, -i, -j, -k\right\}$$

le groupe des quaternions, i.e. avec $i^2 = j^2 = k^2 = -1$ et $ij = k, jk = i$ et $ki = j$.

On note $\mathbb{F}_9 = \mathbb{F}_3[i] = \mathbb{F}_3[X]/\langle X^2 + 1\rangle$ avec $i^2 = -1$. On a alors $S^\times = \{1, -1, i, -i\}$ et $(\pm i)^{\star 2} = i^2 = -1$ et $(\pm 1 \pm i)^{\star 2} = N(i+1) = -1$. Donc $\mathbb{F}_9^\times$ possède 6 éléments d'ordre 4 donc il ne peut être isomorphe à D_4 qui n'en possède que 2 (qui sont τ et τ^3). Donc

$$(\mathbb{F}_9, \star) \simeq Q_8.$$

Proposition 11. *Soit α un générateur de $K^\times$ alors*[6] *$(K^\times, \star) = \langle \alpha, \alpha^2 \rangle$. De plus on a*

1. *Pour tout $a \in S, \mathrm{ord}_\star(a) = \mathrm{ord}(a)$*

6. Attention on considère α un générateur de $(K^\times, \times)$ qui est bien cyclique et dans les générateurs de $(K^\times, \star)$ on a $\alpha^2 = \alpha \times \alpha$ à ne pas confondre avec $\alpha^{\star 2}$.

2. *Pour tout* $a \in K \setminus S, \mathrm{ord}_\star(a) = 2\,\mathrm{ord}(N(a))$

Démonstration. Soit $a \in K^\times$. Puisque $K^\times$ est cyclique il existe un entier n tel que $a = \alpha^n$. Si $n = 2m$ est pair alors $(\alpha^2)^{\star m} = (\alpha^2)^m = a$ car α^2 est un carré. Sinon $n = 2m+1$ et on a alors $\alpha \star (\alpha^2)^{\star m} = \underbrace{\gamma^{\delta(\alpha^{2m})}}_{=\mathrm{id}_K}(\alpha)\alpha^{2m} = \alpha\alpha^{2m} = \alpha^{2m+1}$.

On montre les deux autres affirmations.

1. Soit $a \in S$ alors $a^{\star n} = a^n$ donc l'ordre de a pour la loi $\star$ reste la même que pour $\times$.
2. Soit $a \in K \setminus S$ alors en particulier $a \notin k$. On note $d = \mathrm{ord}_\star(a)$. On a alors $a^{\star 2} = \gamma(a)a = N(a)$ d'après le Lemme 4. Puisque $N(a) \in k \subseteq S$ alors $a^{\star 2n} = N(a)^n$ donc $d | 2\,\mathrm{ord}(N(a))$. D'autre part, toujours d'après le Lemme 4, $a^{\star 2n+1} = N(a)^n a \in K \setminus k$ donc a ne peut être d'ordre impair. On en déduit que $d = 2d'$ pour un certain d et donc $a^{\star 2d'} = N(a)^{d'} = 1$ donc $\mathrm{ord}(N(a)) | d'$ donc $2\,\mathrm{ord}(N(a)) | d$ donc on a bien
$$\mathrm{ord}_\star(a) = 2\,\mathrm{ord}(N(a)).$$

□

Théorème 11. *Soit* $K = \mathbb{F}_{q^2}$ *que l'on munit de la loi* $\star$ *et* $k = \mathbb{F}_q \subseteq K$. *Alors on a un isomorphisme de groupes*
$$K^\times / k^\times \simeq D_{\frac{q+1}{2}}$$
avec $D_{\frac{q+1}{2}}$ *le groupe diédral à* $q+1$ *éléments.*

Démonstration. D'après le Lemme 5 l'image $\overline{S}^\times$ de $S^\times$ dans le quotient $\overline{K}^\times = K^\times / k^\times$ est un sous-groupe distingué d'ordre $\frac{q+1}{2}$. De plus, d'après la Proposition 11, $\overline{K}^\times$ est engendré par les classes $\overline{\beta}$ et $\overline{\alpha}$ de $\beta = \alpha^2$ et de α où α est un générateur de $K^\times$ (munit de la multiplication usuelle). De plus, puisque $\alpha^{\star 2} = N(\alpha) \in k^\times$ on a $M = \langle \overline{\alpha} \rangle$ sous-groupe d'ordre 2 de $\overline{K}^\times$.

On a donc bien $M\overline{S}^\times = \overline{K}^\times$ et $M \cap \overline{S}^\times = \{1\}$ donc $(\overline{K}^\times, \star)$ est le produit semi-direct $\overline{S}^\times \rtimes M$. Le morphisme définissant le produit est

$$\begin{array}{rccc} f\colon & M & \longrightarrow & \mathrm{Aut}\left(\overline{S}^\times\right) \\ & 1 & \longmapsto & \mathrm{id} \\ & \alpha & \longmapsto & (\overline{s} \mapsto \overline{\alpha} \star \overline{s} \star \overline{\alpha} = \overline{\gamma(s)}) \end{array}$$

Puisque $S^\times \setminus k^\times$ n'est jamais vide, f n'est jamais constant et donc le produit semi-direct n'est pas direct. Il s'agit donc bien du groupe diédral comme énoncé dans le théorème. □