

Proyecciones  
Vol. 24, N° 3, pp. 181-203, December 2005.  
Universidad Católica del Norte  
Antofagasta - Chile

## UNE PROPRIÉTÉ DU GROUPE À 168 ÉLÉMENTS

REMI GOBLOT  
*University Mohamed I, Morocco*

*Received : December 2004. Accepted : July 2005*

### Abstract

*Let  $\mathcal{E}$  be an affine space of dimension  $n$  over a field  $K$ ,  $\mathcal{G}$  the affine group of  $\mathcal{E}$ ,  $G$  the corresponding linear group. To each point  $a \in \mathcal{E}$  corresponds a section  $s_a: G \rightarrow \mathcal{G}$  of the canonical map  $\mathcal{G} \rightarrow G$ : to the linear map  $\varphi \in G$  corresponds the affine map  $\varphi_a$  which has  $\varphi$  as associated linear map and  $a$  as fixed point. We prove that every section is of this type, except in the only one case where  $K = \mathbf{F}_2$  and  $n = 3$ .*

Soit  $K$  un corps commutatif,  $\mathcal{E}$  un  $K$ -espace affine de dimension  $n$ ,  $E$  l'espace des vecteurs de  $\mathcal{E}$ ,  $\mathcal{G}$  le groupe affine et  $\mathcal{T}$  le sous-groupe des translations,  $G \sim \mathcal{G}/\mathcal{T}$  le groupe linéaire. Pour  $\varphi \in \mathcal{G}$ , on note  $\overline{\varphi}$  l'application linéaire associée dans  $G$ . Pour  $f \in G$  et  $a \in \mathcal{E}$ , on note  $f_a$  l'application affine fixant  $a$  d'application linéaire associée  $f$ . À tout  $a \in \mathcal{E}$  correspond donc la section

$$s_a: G \hookrightarrow \mathcal{G}, f \mapsto f_a$$

L'objet de ce travail est de montrer le théorème suivant:

**Théorème** a) Toute section  $s: G \rightarrow \mathcal{G}$  est du type  $s_a$  à l'exception du cas où  $K = \mathbf{F}_2$  et  $n = 3$ .

b) On suppose  $K = \mathbf{F}_2$  et  $n = 3$ . Soit  $\mathcal{F}$  l'ensemble des sous-groupes de  $G$  de cardinal 7. Pour tout  $M \in \mathcal{F}$ , soit  $N(M)$  le normalisateur de  $M$ . L'ensemble  $\mathcal{F}$  est muni d'une structure canonique de  $\mathbf{F}_2$ -espace affine de dimension 3 d'espace des vecteurs  $E$ : pour  $M_1$  et  $M_2$  distincts de  $\mathcal{F}$ ,  $N(M_1) \cap N(M_2) = \{I, g, g^2\}$  est un sous-groupe de  $G$  d'ordre 3. On pose  $\overrightarrow{M_1 M_2} = \overrightarrow{\varepsilon}$  où  $\overrightarrow{\varepsilon}$  est le vecteur de  $E$  fixe par  $g$ . L'opération de  $G$  sur  $\mathcal{F}$  par conjugaison donne une section de  $G$  dans le groupe affine de  $\mathcal{F}$  sans point fixe.

c) L'ensemble  $\mathcal{E}'$  des isomorphismes affines  $\mathcal{E} \rightarrow \mathcal{F}$  induisant l'identité sur  $E$  a une structure canonique de  $\mathbf{F}_2$ -espace affine de dimension 3 de même espace vectoriel associé  $E$  et de même groupe affine  $\mathcal{G}$  que  $\mathcal{E}$ . L'ensemble des sections  $G \hookrightarrow \mathcal{G}$ , de cardinal 16, est en bijection canonique avec  $\mathcal{E} \cup \mathcal{E}'$ . Les espaces affines  $\mathcal{E}$  et  $\mathcal{E}'$  jouent le même rôle l'un par rapport à l'autre.

**Cas où  $K$  n'est pas  $\mathbf{F}_2$**  . Montrons que toute section est du type  $s_a$  où  $a \in \mathcal{E}$ .

Soit  $s$  une section et  $\lambda \neq 1$  dans  $K^\times$ . L'homothétie vectorielle  $\lambda I_E$  se remonte par  $s$  en une homothétie affine  $hom(a, \lambda)$  de rapport  $\lambda$  et de centre  $a$ . Soit  $f \in G$  et  $\varphi = s(f)$ . L'homothétie vectorielle  $\lambda I_E$  commute avec  $f$ , donc  $s(\lambda I_E) = hom(a, \lambda)$  commute avec  $s(f) = \varphi$ . On a donc

$$\varphi(a) = (\varphi \circ hom(a, \lambda))(a) = (hom(a, \lambda) \circ \varphi)(a) = (hom(a, \lambda))(\varphi(a))$$

Comme  $a$  est seul point fixe de  $hom(a, \lambda)$ , on a  $\varphi(a) = a$  et  $s$  est la section  $s_a$  envoyant  $G$  en le stabilisateur de  $a$ .

Ce raisonnement tombe en défaut si  $K = \mathbf{F}_2$  car il n'existe aucun  $\lambda \neq 1$ . Dans la suite, le corps est  $\mathbf{F}_2$  et  $\dim E = 3$ . Dans la section 1, on étudie les sous-groupes de  $G$ . Les sections 2 et 3 développent respectivement les

points  $b$ ) et  $c$ ) du théorème. La section 4 envisage le cas des  $\mathbf{F}_2$ -espaces vectoriels de dimension supérieure 3.

### 1. Sous groupes du groupe $G$

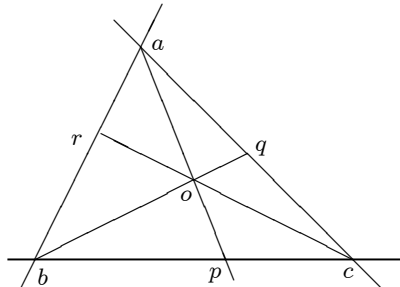
**1.1 Plans projectifs sur  $\mathbf{F}_2$**  . Le cardinal de  $G$  est  $7 \times 6 \times 4 = 168$ , nombre de bases de  $E$ . Le groupe multiplicatif  $\mathbf{F}_2^\times$  étant réduit à  $\{1\}$ , la géométrie vectorielle sur  $E$  et la géométrie projective sur le plan projectif  $P(E)$  se confondent: on a une bijection canonique

$$E \setminus \{\vec{0}\} \rightarrow P(E) , \vec{v} \mapsto v$$

On notera de la même façon une application linéaire inversible  $f: E \rightarrow E$  et l'homographie  $f: P(E) \rightarrow P(E)$  associée. La donnée d'une base  $(\vec{e}_1, \vec{e}_2, \vec{e}_3)$  de  $E$  équivaut à la donnée d'un triangle non aplati  $(e_1, e_2, e_3)$  de  $P(E)$ , qui se complète d'une façon unique en un repère  $(e_1, e_2, e_3, e_4)$  de  $P(E)$  où  $e_4$  est l'unique point de  $P(E)$  ne se trouvant sur aucun des côtés du triangle. Une homographie est donc définie par la donnée d'un triangle et du triangle image.

Le plan projectif  $P(E)$  comporte 7 points et 7 droites. Par chaque point passent 3 droites et chaque droite porte 3 points. La figure suivante constituée d'un triangle  $abc$  et de 3 droites  $(ap), (bq), (cr)$  concourantes en  $o$  permet de se représenter un plan projectif sur  $\mathbf{F}_2$  en convenant de considérer  $p, q, r$  comme alignés.

L'ensemble des 7 droites de  $P(E)$  constitue le plan projectif dual  $P(E^*) = P^*(E)$ .



**Proposition 1.** Soit  $P$  un ensemble de points,  $P^*$  un ensemble de cardinal supérieur à 1 de droites.

On suppose vérifiées les conditions d'incidence suivantes:

- pour toute droite, exactement trois points sont en incidence avec cette droite
- pour toute paire de deux points distincts, une unique droite est en incidence avec ces deux points,
- pour toute paire de deux droites distinctes, un unique point est en incidence avec ces deux droites.

Alors  $P$  a une structure de  $\mathbf{F}_2$ -plan projectif et  $P^*$  s'identifie à l'ensemble des droites de  $P$ . Une bijection  $h: P \rightarrow P$  est une homographie si et seulement si elle conserve l'alignement.

Montrons qu'un point  $o$  est en incidence avec exactement 3 droites. Soit  $m_1$  distinct de  $o$ . Comme  $(om_1)$  n'est pas la seule droite, il existe  $m_2 \notin (om_1)$ . Soit  $m_3$  le troisième point de la droite  $D = (m_1m_2)$ .

Les droites  $(om_1)$ ,  $(om_2)$ ,  $(om_3)$  sont en incidence avec  $o$ . Une quatrième droite couperait  $D$  en un quatrième point ce qui est impossible. Pour tout  $i \in \{1, 2, 3\}$ , soit  $m'_i$  le troisième point de  $(om_i)$ , alors

$P = \{o, m_1, m'_1, m_2, m'_2, m_3, m'_3\}$  est de cardinal 7.

Adjoignons un élément  $\vec{0}$  à  $P$ . Un élément sera noté  $x$  ou  $\vec{x}$  selon qu'on le considère comme appartenant à  $P$  ou à  $E = P \cup \{\vec{0}\}$ . On définit sur  $E$  l'addition suivante:

- $\forall \vec{x} \in E$ ,  $\vec{x} + \vec{0} = \vec{0} + \vec{x} = \vec{x}$ ,
- $\forall \vec{x} \in E$ ,  $\vec{x} + \vec{x} = \vec{0}$ ,
- pour  $\vec{x}$  et  $\vec{y}$  distincts de  $\vec{0}$  et entre eux,  $\vec{x} + \vec{y} = \vec{z}$  où  $z$  est le troisième point de la droite en incidence avec  $x$  et  $y$ .

Cette addition est associative:  $(\vec{\alpha} + \vec{\beta}) + \vec{\gamma} = \vec{\alpha} + (\vec{\beta} + \vec{\gamma})$ . Montrons le si  $\alpha, \beta, \gamma$  sont distincts non alignés. Soit  $\vec{\delta} = \vec{\alpha} + \vec{\beta}$  et  $\vec{\varepsilon} = \vec{\beta} + \vec{\gamma}$  et  $\sigma$  l'unique point en incidence avec les droites  $(\delta\gamma)$  et  $(\alpha\varepsilon)$ . On a

$$(\vec{\alpha} + \vec{\beta}) + \vec{\gamma} = \vec{\delta} + \vec{\gamma} = \vec{\sigma} \quad \text{et} \quad \vec{\alpha} + (\vec{\beta} + \vec{\gamma}) = \vec{\alpha} + \vec{\varepsilon} = \vec{\sigma}$$

Alors  $E$ , de cardinal 8, a une structure de  $\mathbf{F}_2$ -espace vectoriel de dimension 3,  $P$  s'identifie au plan  $P(E)$  et  $P^*$  au dual de  $P$ .

Montrons qu'une bijection  $h: P \rightarrow P$  conservant l'alignement est une homographie. On prolonge  $h$  à  $E$  en posant  $h(\vec{0}) = \vec{0}$ . Soit  $\vec{x}, \vec{y}$

non nuls et distincts,  $\vec{z} = \vec{x} + \vec{y}$ . Alors  $x, y, z$  sont alignés distincts, donc  $h(x), h(y), h(z)$  sont alignés distincts, d'où  $h(\vec{x}) + h(\vec{y}) = h(\vec{z})$  et  $h: E \rightarrow E$  est bien linéaire.

**1.2 Sous-groupes isomorphes à  $\mathbf{S}_4$**  . Soit  $D$  une droite de  $P(E)$ . L'ensemble  $P(E) \setminus D$ , formé de quatre points, est un repère projectif de  $P(E)$ . Considérant l'action du stabilisateur  $St(D)$  de  $D$  sur le quadrilatère  $P(E) \setminus D$ , on obtient un isomorphisme  $St(D) \sim \mathbf{S}_4$ . Soit  $G(D) \sim \mathbf{S}_3$  le groupe des homographies de  $D$ . L'application *restriction à  $D$*  définit un morphisme  $St(D) \sim \mathbf{S}_4 \rightarrow \mathbf{G}(D) \sim \mathbf{S}_3$  dont le noyau est un groupe de Klein  $Kl(D)$ : l'ensemble des  $h \in G$  induisant l'identité sur  $D$ . Ce groupe  $Kl(D)$  est formé de l'identité et de trois involutions, chacune induisant deux transpositions disjointes sur le quadrilatère  $P(E) \setminus D$ . On a 7 droites dans  $P(E)$ , une classe de conjugaison de 7 groupes  $St(D)$  et une classe de conjugaison de 7 groupes de Klein  $Kl(D)$ .

Dualement, le stabilisateur  $St(m)$  d'un point  $m$  est isomorphe à  $\mathbf{S}_4$ . Le sous-groupe de Klein  $Kl(m)$  est formé des homographies laissant stable chacune des trois droites passant par  $m$ . Une involution de  $Kl(m)$  laisse fixe les points d'une de ces trois droites et échange les deux points distincts de  $m$  sur chacune des deux autres. On a 7 points dans  $P(E)$ , une classe de conjugaison de 7 groupes  $St(m)$  et une classe de conjugaison de 7 groupes de Klein  $Kl(m)$ .

**1.3 Sous-groupes d'ordre 8 et involutions** . Il s'agit de la classe de conjugaison des 2-Sylow(s). Dans chaque groupe isomorphe à  $\mathbf{S}_4$ , on a trois sous-groupes diédraux de cardinal 8. Un 2-Sylow est donc contenu dans  $St(D) \cap St(m)$  où  $D$  est une droite et  $m$  un point. Nécessairement,  $m \in D$ , sinon  $m$  est un point du repère  $P(E) \setminus D$  et  $St(D) \cap St(m) \sim \mathbf{S}_3$  est le stabilisateur de  $m$  dans  $St(D) \sim \mathbf{S}_4$ .

Un 2-Sylow est donc le stabilisateur  $St(D, m)$  d'un couple  $(D, m)$  où  $D$  est une droite et  $m$  un point de  $D$ . On a 7 droites et sur chacune 3 points, d'o 21 couples  $(D, m)$ . La classe de conjugaison des 2-Sylow(s) est de cardinal 21.

Toute involution étant contenue dans un 2-Sylow, les involutions de  $G$  sont celles mises en évidence précédemment: ce sont des paires de transpositions disjointes  $(a, b), (c, d)$  où le quadrilatère  $a, b, c, d$  est un repère projectif de  $P(E)$ . On a 7 tels quadrilatères et pour chacun d'eux 3 telles involutions. Les involutions de  $G$  forment une classe de conjugaison de cardinal 21.

On a une bijection canonique de l'ensemble des 21 2-Sylo(s) sur l'ensemble des 21 involutions: à tout 2-Sylo  $St(D, m)$ , on associe l'involution  $\tau_{D,m}$  telle que  $\{I, \tau_{D,m}\}$  soit le centre de  $St(D, m)$ . Si  $a, b, c, d$  sont les 4 points de  $P(E) \setminus D$ , choisissant les notations de sorte que les droites  $(ab)$  et  $(cd)$  se coupent en  $m$ , alors  $\tau_{D,m}$  échange  $a$  et  $b$  et échange  $c$  et  $d$ . On a  $\{I, \tau_{D,m}\} = Kl(D) \cap Kl(m)$ .

**1.4 Sous-groupes d'ordre 3 et 6** . Soit  $D$  une droite. Alors  $P(E) \setminus D$  est un quadrilatère et le groupe  $St(D)$  est isomorphe à  $\mathbf{S}_4$ . tout  $m \in P(E) \setminus D$  est associé le groupe  $St(D, m) \sim \mathbf{S}_3$  laissant stables  $D$  et  $m$  et le sous-groupe  $\Gamma(D, m) \sim \mathbf{A}_3$  formé de deux permutations circulaires sur les 3 points de  $D$  et sur les 3 points du triangle complémentaire de  $D \cup \{m\}$ . Les groupes  $\Gamma(D, m)$  sont des 3-Sylo(s). Les 3-Sylo(s) étant conjugués, ils sont tous de ce type.

On a 7 possibilités pour la droite  $D$  et  $7 - 3 = 4$  possibilités pour le point  $m \notin D$ , d'où  $7 \times 4 = 28$  sous-groupes du type  $St(D, m) \sim \mathbf{S}_3$  et 28 sous-groupes  $\Gamma(D, m) \sim \mathbf{A}_3$ .

**1.5 Les deux classes de conjugaison des groupes isomorphes à  $\mathbf{S}_4$  comme  $\mathbf{F}_2$ -plans projectifs en dualité** . Les sous-groupes de  $G$  isomorphes à  $\mathbf{S}_4$  se rangent en deux classes de conjugaison: les 7 stabilisateurs de point  $St(m)$  où  $m \in P$ , les 7 stabilisateurs de droite  $St(D)$  où  $D \in P^*$ . On a les relations d'incidence:

- Soit  $A, B$  deux droites distinctes se coupant en  $m$ ,  $C$  la troisième droite passant par  $m$ . On a  $St(A) \cap St(B) = St(C, m) = \{I, \tau_{C,m}\}$ . De même, soit  $a, b$  deux points distincts de  $P(E)$ ,  $c$  le troisième point de la droite  $D = (ab)$ . Alors  $St(a) \cap St(b) = St(D, c) = \{I, \tau_{D,c}\}$ .
- Soit  $D$  une droite,  $m \notin D$  un point, alors  $St(D) \cap St(m) = St(D, m) \sim S_3$ .
- Soit  $D$  une droite,  $m \in D$  un point, alors  $St(D) \cap St(m) = St(D, m)$  est diédral de cardinal 8.

**Proposition 2.** Soit  $P, P^*$  les deux classes de conjugaison de sous-groupes isomorphes à  $\mathbf{S}_4$ . Soit  $S, S'$  deux sous-groupes de  $P \cup P^*$ .

- $S \cap S'$  est de cardinal 2 si et seulement si  $S$  et  $S'$  sont dans la même classe de conjugaison.

- $S \cap S' \sim \mathbf{S}_3$  si et seulement si  $S$  et  $S'$  ne sont pas dans la même classe de conjugaison et ne sont pas en incidence.
- $S \cap S'$  est diédral de cardinal 8 si et seulement si  $S$  et  $S'$  ne sont pas dans la même classe de conjugaison et sont en incidence.

**1.6 Sous-groupes d'ordre 7 de  $G$**  . Ils forment l'ensemble  $\mathcal{F}$  des 7-Sylow(s). Raisonnons dans le cadre vectoriel. L'extension  $\mathbf{F}_8$  de  $\mathbf{F}_2$  est une  $\mathbf{F}_2$ -algèbre de rang 3. Le groupe multiplicatif  $\mathbf{F}_8^\times$  est cyclique d'ordre 7. Les éléments de  $\mathbf{F}_8^\times$  se rangent en deux classes  $x, x^2, x^4$  et  $x^{-1}, x^{-2}, x^{-4}$ , racines des deux polynômes irréductibles de degré 3:

$$P(X) = X^3 + X + 1 \quad , \quad Q(X) = X^3 + X^2 + 1$$

Dans  $G$ , on a deux classes  $\mathcal{P}$  et  $\mathcal{Q}$  d'éléments d'ordre 7 selon que le polynôme minimal est  $P(X)$  ou  $Q(X)$ .

Soit  $\mathcal{B}(E)$  l'ensemble des bases de  $E$ . On a une application  $\mathcal{B}(E) \rightarrow \mathcal{P}$  associant à la base  $(\vec{e}_1, \vec{e}_2, \vec{e}_3)$  l'application dont la matrice dans cette base est la matrice compagnon de  $P(X)$ :

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

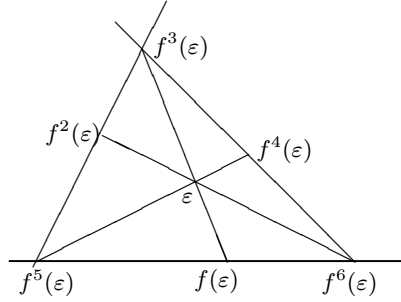
Cette application est surjective. En effet, soit  $f$  admettant  $P(X)$  pour polynôme caractéristique. Comme  $P(X)$  est irréductible,  $f$  n'a aucun vecteur propre et admet la matrice compagnon de  $P(X)$  dans toute base  $(\vec{e}_1, f(\vec{e}_1), f^2(\vec{e}_1))$ . Ainsi,  $\mathcal{P}$  et  $\mathcal{Q}$  sont les deux classes de conjugaison des éléments d'ordre 7 de  $G$ .

Soit  $\vec{e}_1 \neq \vec{0}$ . L'application  $f \mapsto (f(\vec{e}_1), f^2(\vec{e}_1))$  est donc une bijection de  $\mathcal{P}$  sur l'ensemble des couples de vecteurs  $(\vec{e}_2, \vec{e}_3)$  tels que  $(\vec{e}_1, \vec{e}_2, \vec{e}_3)$  soit base de  $E$ . On a  $8 - 2 = 6$  possibilités pour  $\vec{e}_2$  et  $8 - 4 = 4$  possibilités pour  $\vec{e}_3$ .

Ainsi,  $Card\mathcal{P} = 6 \times 4 = 24$ . Les éléments de  $\mathcal{P}$  se rangent en 8 paquets de 3 éléments  $(f, f^2, f^4)$  engendrant le même groupe  $M = \langle f \rangle = \langle f^2 \rangle = \langle f^4 \rangle$  d'ordre 7. L'ensemble  $\mathcal{F}$  des sous-groupes d'ordre 7 est donc de cardinal 8.

Considérons un tel sous-groupe  $M$  et ses générateurs  $f, f^2, f^4$  appartenant à  $\mathcal{P}$ . Comme le coefficient de  $X^2$  dans  $P$  est nul, pour tout  $\vec{e} \neq$

$\vec{0} \in E$ , on a  $f(\vec{\varepsilon}) + f^2(\vec{\varepsilon}) + f^4(\vec{\varepsilon}) = \vec{0}$ . Considérant la droite vectorielle  $\Delta = \{\vec{0}, \vec{\varepsilon}\}$  et le plan vectoriel  $\Pi = \{\vec{0}, f(\vec{\varepsilon}), f^2(\vec{\varepsilon}), f^4(\vec{\varepsilon})\}$ , on a  $E = \Delta \oplus \Pi$ . La donnée du groupe  $M = \langle f \rangle = \langle f^2 \rangle = \langle f^4 \rangle$  induit une orientation sur le plan  $\Pi$  en prenant la permutation circulaire  $(f(\vec{\varepsilon}), f^2(\vec{\varepsilon}), f^4(\vec{\varepsilon}))$ , indépendante du générateur  $f \in \text{cal}P \cap M$ . Ainsi, la donnée d'un  $M \in \mathcal{F}$  détermine 7 décompositions orientées  $E = \Delta \oplus \Pi$  où  $\Delta = \{\vec{0}, \vec{\varepsilon}\}$  et  $\Pi = \{\vec{0}, f(\vec{\varepsilon}), f^2(\vec{\varepsilon}), f^4(\vec{\varepsilon})\}$  muni de la permutation circulaire  $(f(\vec{\varepsilon}), f^2(\vec{\varepsilon}), f^4(\vec{\varepsilon}))$  avec  $f \in \mathcal{P} \cap M$ .



Pour tout  $k \in \mathbf{Z}$ , les points  $f^k(\varepsilon), f^{k+1}(\varepsilon), f^{k+3}(\varepsilon)$  sont alignés.

## 2. Structure d'espace affine sur $\mathcal{F}$

**2.1 Sous-groupes d'ordre 21** . Soit  $M$  un sous-groupe d'ordre 7. Formons le *normalisateur*  $N(M)$ , plus grand sous-groupe dans lequel  $M$  est distingué.

Le groupe  $M$  concide avec son commutant. En effet, si  $h$  commute avec  $f \in \text{cal}P \cap M$ , comme le polynôme minimal de  $f$  est  $P(X)$ , de degré 3, donc égal au polynôme caractéristique,  $E$  est cyclique pour  $f$  et  $h$  appartient à l'algèbre  $\mathbf{F}_2[f] \sim \mathbf{F}_2[\mathbf{X}]/(\mathbf{P}) \sim \mathbf{F}_8$  des applications linéaires polynomiales en  $f$ . Cette algèbre se déduit de  $M$  par adjonction de l'application nulle.

Soit  $g \in N(M)$ . L'automorphisme  $h \mapsto ghg^{-1}$  laisse  $P \cap M = \{f, f^2, f^4\}$  stable.

Si cet automorphisme laisse fixe un élément de  $\{f, f^2, f^4\}$ , on peut supposer que c'est  $f$ . On a alors  $gf = fg$ , donc  $g \in M$ .

Si  $g \notin M$ , cet automorphisme induit une permutation circulaire sur  $\{f, f^2, f^4\}$  et  $g^3 \in M$ . Comme  $g$  opère sur  $P(E)$  de cardinal 7, en le décomposant en cycles disjoints, on voit que son ordre ne peut être 21, donc est nécessairement 3. Deux cas sont à envisager:



- $gf g^{-1} = f^2$  ,  $gf^2 g^{-1} = f^4$  ,  $gf^4 g^{-1} = f$  ,
- $gf g^{-1} = f^4$  ,  $gf^2 g^{-1} = f$  ,  $gf^4 g^{-1} = f^2$ .

**Définition.** On dira que  $g$  est *relié* à  $M$  dans le premier cas. Il s'agit bien d'une relation entre  $g$  et  $M$  car si elle est vraie pour un  $f \in \text{cal}P \cap M$ , elle est aussi vraie pour les autres éléments  $f^2, f^4$  de  $\text{cal}P \cap M$ .

Supposons  $g$  relié à  $M$ . Soit  $\varepsilon$  le point fixe de  $g$ . Les relations  $g(\varepsilon) = \varepsilon$ ,  $gf = f^2g$ ,  $gf^2 = f^4g$ ,  $gf^4 = fg$  impliquent que  $gf(\varepsilon) = f^2(\varepsilon)$ ,  $gf^2(\varepsilon) = f^4(\varepsilon)$ ,  $gf^4(\varepsilon) = f(\varepsilon)$ . Autrement dit, la droite stable par  $g$  est  $\{f(\varepsilon), f^2(\varepsilon), f^4(\varepsilon)\}$ .

Inversement, soit un point  $\varepsilon \in P(E)$  et la droite  $\{f(\varepsilon), f^2(\varepsilon), f^4(\varepsilon)\}$ . Définissons  $g$  par  $g(\varepsilon) = \varepsilon$ ,  $g(f(\varepsilon)) = f^2(\varepsilon)$ ,  $g(f^2(\varepsilon)) = f^4(\varepsilon)$ . Comme  $g$  respecte l'alignement, on a  $g(f^4(\varepsilon)) = f(\varepsilon)$ ,  $g(f^3(\varepsilon)) = f^6(\varepsilon)$ ,  $g(f^6(\varepsilon)) = f^5(\varepsilon)$ ,  $g(f^5(\varepsilon)) = f^3(\varepsilon)$ . D'où l'on déduit que  $g \in N(M)$  est relié à  $M$ . On a donc autant d'éléments  $g$  d'ordre 3 reliés à  $M$  que de points  $\varepsilon \in P(E)$ , c'est-à-dire 7. Leurs carrés  $g^2$  sont les 7 autres éléments d'ordre 3 de  $N(M)$ .

Remarquons que la donnée d'un groupe  $M$  d'ordre 7 détermine sur  $P(E)$  une structure de  $\mathbf{F}_7$ -droite affine pour laquelle  $M$  est le groupe des translations. Le groupe  $N(M)$ , de cardinal 21, apparaît alors comme groupe des homothéties-translations de rapport 1, 2, 4 (les carrés de  $\mathbf{F}_7$ ). C'est le produit semi-direct de  $M$  par chacun de ses 7 sous-groupes d'ordre 3 (Cf. 1.7).

Un élément  $g$  d'ordre 3 est relié à un unique sous-groupe d'ordre 7. En effet, soit  $\varepsilon$  le point fixe de  $g$ ,  $\{e, g(e), g^2(e)\}$  la droite laissée stable par  $g$ , alors  $g$  est relié au groupe  $M = \langle f \rangle$  où  $f(\varepsilon) = e$ ,  $f^2(\varepsilon) = g(e)$ ,  $f^4(\varepsilon) = g^2(e)$ . Remplacer  $f$  par  $f^2$  ou  $f^4$  revient à faire une permutation circulaire sur  $e, g(e), g^2(e)$ . Ceci se résume dans la définition et la proposition suivantes

**Définition.** Soit  $M$  un groupe d'ordre 7,  $P \cap M = (f, f^2, f^4)$ . Un élément  $g$  d'ordre 3 est relié à  $M$  s'il vérifie les trois conditions (équivalentes) suivantes:

$$(gf g^{-1} = f^2) \iff (gf^2 g^{-1} = f^4) \iff (gf^4 g^{-1} = f)$$

**Proposition 3.** Tout élément  $g$  d'ordre 3 est relié à un unique groupe  $M$  d'ordre 7. Si  $\varepsilon \in P$  est le point fixe de  $g$  et si  $\text{cal}P \cap M = (f, f^2, f^4)$ , alors  $(f(\varepsilon), f^2(\varepsilon), f^4(\varepsilon))$  est la droite stable par  $g$ .

Le groupe  $\langle g \rangle = \langle g^2 \rangle$  d'ordre 3, de point fixe  $\varepsilon$ , est relié à deux groupes  $M_1$  et  $M_2$  d'ordre 7 où, avec  $\text{cal}P \cap M = (f_1, f_1^2, f_1^4)$  et  $\text{cal}P \cap M_2 = (f_2, f_2^2, f_2^4)$ , on a

$$\begin{aligned} f_1(\varepsilon) &= e, \quad f_1^2(\varepsilon) = g(e), \quad f_1^4(\varepsilon) = g^2(e) \\ f_2(\varepsilon) &= e, \quad f_2^2(\varepsilon) = g^2(e), \quad f_2^4(\varepsilon) = g(e) \end{aligned}$$

**2.2 Les 28 3-sylow(s) et les 28 paires de 7-sylow(s)** . Á tout élément  $g \in G$  d'ordre 3, on associe le point fixe  $\varepsilon$  et la droite stable orientée  $(e, g(e), g^2(e))$ , puis les trois éléments  $f_1, f_1^2, f_1^4$  d'ordre 7 appartenant à  $\mathcal{P}$  définis par

$$f_1(\varepsilon) = e, \quad f_1^2(\varepsilon) = g(e), \quad f_1^4(\varepsilon) = g^2(e)$$

On a ainsi une application  $g \mapsto M(g)$  de l'ensemble des 56 éléments d'ordre 3 sur l'ensemble  $\mathcal{F}$  des 8 sous-groupes d'ordre 7.

**Proposition 4.** (i) L'application de l'ensemble des 28 sous-groupes d'ordre 3 dans l'ensemble des paires de sous-groupes distincts d'ordre 7

$$(I, g, g^2) \mapsto (M(g), M(g^2))$$

est bijective.

(ii) Étant donné deux couples  $(M_1, M_2)$  et  $(M'_1, M'_2)$  d'éléments de  $\mathcal{F}$  où  $M_1 \neq M_2$  et  $M'_1 \neq M'_2$ , l'ensemble des  $h \in G$  tels que  $hM_i h^{-1} = M'_i$  pour  $i \in \{1, 2\}$  est de cardinal 3.

(i) C'est une application de l'ensemble des 28 sous-groupes d'ordre 3 dans l'ensemble des  $C_8^2 = 28$  paires  $(M_1, M_2)$  de sous-groupes distincts de  $\mathcal{F}$ : à  $\Gamma = (I, g, g^2)$  on associe la paire  $(M(g), M(g^2))$ , avec  $M(g) = \langle f_1 \rangle$  et  $M(g^2) = \langle f_2 \rangle$  où,  $\varepsilon$  étant le point fixe de  $g$  et  $g^2$ ,

$$f_1(\varepsilon) = e, \quad f_1^2(\varepsilon) = g(e), \quad f_1^4(\varepsilon) = g^2(e)$$

$$f_2(\varepsilon) = e, \quad f_2^2(\varepsilon) = g^2(e), \quad f_2^4(\varepsilon) = g(e)$$

Pour montrer la bijectivité de cette application, il suffit de voir l'injectivité. Pour  $g$  d'ordre 3, les groupes  $M(g) = M_1$  et  $M(g^2) = M_2$  sont distincts et  $\Gamma = (I, g, g^2)$  est dans l'intersection des normalisateurs  $N(M_1) \cap N(M_2)$ .

S'agissant de groupes de cardinal 21, cette intersection ne peut être que de cardinal 3, donc réduite à  $\Gamma$  qui est donc l'unique antécédent de  $(M_1, M_2)$ .

(ii) On forme  $N(M_1) \cap N(M_2) = (I, g, g^2)$  et  $N(M'_1) \cap N(M'_2) = (I, g', g'^2)$  où  $g$  (resp.  $g^2$ ) est relié à  $M_1$  (resp.  $M_2$ ) et  $g'$  (resp.  $g'^2$ ) est relié à  $M'_1$  (resp.  $M'_2$ ). Comme  $M_1$  (resp.  $M'_1$ ) est l'unique groupe de  $\mathcal{F}$  relié à  $g$  (resp.  $g'$ ), l'ensemble des  $h$  cherché est exactement l'ensemble

$$(h \in G \mid g' = hgh^{-1})$$

Il est bien de cardinal 3 car le commutant d'un élément  $g \in G$  d'ordre 3 est  $\langle g \rangle = (I, g, g^2)$  de cardinal 3.

En particulier, l'ensemble des  $s \in G$  tels que  $M_2 = sM_1s^{-1}$  et  $M_1 = sM_2s^{-1}$  est constitué des trois involutions du normalisateur  $N(\Gamma) \sim \mathbf{S}_3$  où  $\Gamma = \langle g \rangle = N(M_1) \cap N(M_2)$ .

**2.3 Structure de  $\mathbf{F}_2$ -espace affine** . Soit  $M_1$  et  $M_2$  deux groupes distincts de  $\mathcal{F}$ . L'intersection des normalisateurs  $N(M_1) \cap N(M_2)$  est un groupe  $\Gamma$  d'ordre 3. Si  $\varepsilon$  est le point laissé fixe par  $\Gamma$ , on pose  $\overrightarrow{M_1M_2} = \overrightarrow{M_2M_1} = \overrightarrow{\varepsilon} \in E$ .

Il s'agit de montrer la *relation de Chasles*: si  $M, M_1, M_2$  sont trois points distincts de  $\mathcal{F}$ , alors

$$\overrightarrow{M_1M_2} = \overrightarrow{M_1M} + \overrightarrow{MM_2}$$

Il existe  $g_1$  et  $g_2$  d'ordre 3 tels que  $g_1$  et  $g_2$  soient tous deux reliés à  $M$ ,  $g_1^2$  relié à  $M_1$  et  $g_2^2$  relié à  $M_2$ . Autrement dit,

$$\Gamma_1 = N(M) \cap N(M_1) = (I, g_1, g_1^2) \quad , \quad \Gamma_2 = N(M) \cap N(M_2) = (I, g_2, g_2^2)$$

pour  $f \in \text{cal}P \cap M$ ,  $f_1 \in \mathcal{P} \cap M_1$ ,  $f_2 \in \mathcal{P} \cap M_2$ , on a

$$g_1fg_1^{-1} = g_2fg_2^{-1} = f^2 \quad , \quad g_1^2f_1g_1^{-2} = f_1^2 \quad , \quad g_2^2f_2g_2^{-2} = f_2^2$$

Si  $\varepsilon_1$  et  $\varepsilon_2$  sont les points fixes de  $g_1$  et  $g_2$ , on a  $\overrightarrow{MM_1} = \overrightarrow{\varepsilon_1}$  et  $\overrightarrow{MM_2} = \overrightarrow{\varepsilon_2}$ .

On va montrer qu'il existe deux couples d'involutions  $(s'_1, s'_2)$  et  $(s''_1, s''_2)$  dans  $N(\Gamma_1) \times N(\Gamma_2)$  tels que  $s' = s'_1s'_2 = s'_2s'_1$  et  $s'' = s''_1s''_2 = s''_2s''_1$  soient des involutions. On aura alors  $M_2 = s'M_1s' = s''M_1s''$ . On vérifiera que  $g = s's''$  est d'ordre 3 appartenant à  $N(M_1) \cap N(M_2)$ . Si  $\varepsilon$  est le point fixe de  $g$ , on aura  $\overrightarrow{M_1M_2} = \overrightarrow{\varepsilon}$ . On vérifiera alors la relation de Chasles:  $\overrightarrow{\varepsilon_1} + \overrightarrow{\varepsilon_2} + \overrightarrow{\varepsilon} = \overrightarrow{0}$ .

Soit  $e \in P(E)$ . Il existe  $i$  et  $j$  tels que  $\varepsilon_1 = f^i(e)$  et  $\varepsilon_2 = f^j(e)$ . Les droites stables de  $g_1$  et  $g_2$  sont respectivement  $(f^{i+1}(e), f^{i+2}(e), f^{i+4}(e))$  et  $(f^{j+1}(e), f^{j+2}(e), f^{j+4}(e))$ . Ces droites ont un point commun. On peut choisir le générateur  $f \in \mathcal{P} \cap M$  et les indices 1 et 2 de sorte que ce point commun soit  $f^{i+2}(e) = f^{j+1}(e)$ , i.e. que  $j = i + 1$ . Pour alléger les notations, on pose  $e_k = f^k(e)$ . Alors  $g_1$  et  $g_2$  ont les décompositions en cycles disjoints

$$g_1 = (e_i)(e_{i+1}, e_{i+2}, e_{i+4})(e_{i+3}, e_{i+6}, e_{i+5})$$

$$g_2 = (e_{i+1})(e_{i+2}, e_{i+3}, e_{i+5})(e_{i+4}, e_i, e_{i+6})$$

On trouve alors dans les normalisateurs de  $\Gamma_1$  et  $\Gamma_2$  les involutions, chacune composée de deux transpositions disjointes

$$s'_1 = (e_{i+2}, e_{i+4})(e_{i+6}, e_{i+5}), \quad s'_2 = (e_{i+2}, e_{i+5})(e_{i+4}, e_{i+6})$$

$$s''_1 = (e_{i+1}, e_{i+4})(e_{i+3}, e_{i+5}), \quad s''_2 = (e_{i+3}, e_{i+5})(e_i, e_{i+6})$$

On a alors

$$s' = s'_1 s'_2 = s'_2 s'_1 = (e_{i+2}, e_{i+6})(e_{i+4}, e_{i+5})$$

$$s'' = s''_1 s''_2 = s''_2 s''_1 = (e_i, e_{i+6})(e_{i+4}, e_{i+1})$$

On en déduit l'élément d'ordre 3

$$g = s' s'' = (e_{i+3})(e_i, e_{i+2}, e_{i+6})(e_{i+1}, e_{i+5}, e_{i+4})$$

On a donc  $\overrightarrow{\varepsilon} = \overrightarrow{M_1 M_2} = \overrightarrow{e_{i+3}}$ . D'où

$$\overrightarrow{\varepsilon_1} + \overrightarrow{\varepsilon_2} + \overrightarrow{\varepsilon} = \overrightarrow{e_i} + \overrightarrow{e_{i+1}} + \overrightarrow{e_{i+3}} = \overrightarrow{0}$$

Vérifions que pour tout  $h \in G$ , l'application  $\tilde{h}: M \mapsto h M h^{-1}$  est affine, d'application linéaire associée  $h$ . Soit  $M_1$  et  $M_2$  dans  $\mathcal{F}$ ,  $f_1 \in \mathcal{P} \cap M_1$ ,  $f_2 \in \mathcal{P} \cap M_2$ ,  $g$  d'ordre 3 tels que  $g f_1 g^{-1} = f_1^2$  et  $g^2 f_2 g^{-2} = f_2^2$ . Soit  $\tilde{h}$  l'automorphisme intérieur de  $G$  déduit de  $h$ . On aura  $\tilde{h}(g) \tilde{h}(f_1) \tilde{h}(g)^{-1} = \tilde{h}(f_1)^2$ ,  $\tilde{h}(g)^2 \tilde{h}(f_2) \tilde{h}(g)^{-2} = \tilde{h}(f_2)^2$ . Si  $\varepsilon$  est le point fixe de  $g$ ,  $h(\varepsilon)$  est le point fixe de  $\tilde{h}(g)$ , donc posant  $M'_1 = \tilde{h}(M_1)$  et  $M'_2 = \tilde{h}(M_2)$ , on a bien

$$\overrightarrow{M'_1 M'_2} = h(\overrightarrow{\varepsilon}) = h(\overrightarrow{M_1 M_2})$$

**Remarque** . Le dual  $E^*$  opère canoniquement sur  $\mathcal{F}$  ainsi: étant donné  $M_1, M_2$  de  $\mathcal{F}$ , on forme  $N(M_1) \cap N(M_2) = (I, g, g^2)$ . Au lieu de considérer le vecteur fixe  $\vec{\varepsilon}$  de  $g$ , on considère le plan vectoriel stable et la forme linéaire  $\overleftarrow{u} \in E^*$  dont il est noyau. On pose alors  $\overleftarrow{M_1 M_2} = \overleftarrow{u} \in E^*$ . On obtient une structure de  $\mathbf{F}_2$ -espace affine *duale* de la première. *On n'a pas les mêmes parallélogrammes.*

Soit  $M_1, M_2, M'_1, M'_2$  distincts dans  $\mathcal{F}$ ,  $\langle g \rangle = N(M_1) \cap N(M_2)$ ,  $\langle g' \rangle = N(M'_1) \cap N(M'_2)$ . Si on avait simultanément

$$\overrightarrow{M_1 M_1} = \overrightarrow{M'_1 M'_2} = \vec{\varepsilon} \quad \text{et} \quad \overleftarrow{M_1 M_2} = \overleftarrow{M'_1 M'_2} = \overleftarrow{u}$$

on aurait  $g(\vec{\varepsilon}) = g'(\vec{\varepsilon}) = \vec{\varepsilon}$  et  $g(\ker u) = g'(\ker u) = \ker u$ . Comme  $E = (\vec{\varepsilon}) \oplus \ker u$ , on aurait  $g' = g$  ou  $g' = g^2$ . Par la proposition 3, on aurait  $(M_1, M_2) = (M'_1, M'_2)$ .

### 3. Groupe affine en dimension 3

Soit  $\mathcal{E}$  un  $\mathbf{F}_2$ -espace affine de dimension 3,  $E$  le  $\mathbf{F}_2$ -espace vectoriel associé,  $\mathcal{G}$  le groupe affine,  $G$  le groupe linéaire. Le sous-groupe  $\mathcal{T}$  des translations est formé de l'identité et de 7 translations non nulles qui sont involutives. Les  $\mathbf{F}_2$ -espaces affines  $\mathcal{E}$  et  $\mathcal{F}$  ont le même espace vectoriel associé  $E$ . En revanche, le groupe affine  $\mathcal{G}$  n'opère pas canoniquement sur  $\mathcal{F}$  et il n'existe pas d'isomorphisme canonique reliant  $\mathcal{E}$  et  $\mathcal{F}$ .

**3.1 L'espace affine  $\mathcal{E}'$**  . *L'ensemble  $\mathcal{E}'$  des isomorphismes affines  $\mathcal{E} \rightarrow \mathcal{F}$  induisant l'identité sur l'espace  $E$  des vecteurs est un espace affine de dimension 3 sur  $\mathbf{F}_2$  admettant  $E$  pour espace des vecteurs et  $\mathcal{G}$  pour groupe affine.*

Deux isomorphismes  $\theta_1, \theta_2: \mathcal{E} \rightarrow \mathcal{F}$  se déduisent l'un de l'autre par une translation de vecteur  $\vec{v} \in E$ : pour tout  $m \in \mathcal{E}$ , on a  $\overrightarrow{\theta_1(m)\theta_2(m)} = \vec{v}$ . On pose alors  $\overrightarrow{\theta_1\theta_2} = \vec{v}$ .

Le groupe  $\mathcal{G}$  opère canoniquement sur  $\mathcal{E}'$ : Soit  $\varphi \in \mathcal{G}$ ,  $\overline{\varphi} \in G$  l'application linéaire associée et  $\theta \in \mathcal{E}'$ . On note encore  $\overline{\varphi}$  l'application affine inversible  $M \mapsto \overline{\varphi}M\overline{\varphi}^{-1}$  de  $\mathcal{F}$  sur lui-même. On pose alors  $\varphi(\theta) = \overline{\varphi} \circ \theta \circ \varphi^{-1}$ .

Dans ces conditions,  $\mathcal{E}$  s'identifie canoniquement à l'espace des isomorphismes affines  $\mathcal{E}' \rightarrow \mathcal{F}$  induisant l'identité sur  $E$ : à  $m \in \mathcal{E}$ , on associe l'isomorphisme  $\theta \mapsto \theta(m)$  de  $\mathcal{E}'$  sur  $\mathcal{F}$ .

**3.2 Sous-groupes d'ordre 7 et 21** . Soit  $f \in \mathcal{G}$  tel que  $\bar{f}$  soit d'ordre 7. Alors 1 n'est pas valeur propre donc  $f$  a un unique point fixe  $m \in \mathcal{E}$ . La surjection canonique  $\mathcal{G} \rightarrow G$  induit un isomorphisme  $\langle f \rangle \sim \langle \bar{f} \rangle$ . Ainsi, l'ensemble  $\mathcal{F} \times \mathcal{E}$  s'identifie à l'ensemble  $\mathcal{Q}$  des sous-groupes d'ordre 7 de  $\mathcal{G}$  en posant pour tout  $(M, m) \in \mathcal{F} \times \mathcal{E}$

$$[M, m] = \left( h \in \mathcal{G} \mid h(m) = m \text{ et } \bar{h} \in M \right)$$

Soit  $f$  un générateur de  $[M, m]$ . Pour tout  $g$  du normalisateur  $N[M, m]$ ,  $gfg^{-1} \in [M, m]$ . Comme  $gfg^{-1}$  admet  $g(m)$  pour point fixe,  $m = g(m)$  car  $gfg^{-1}$ , générateur de  $[M, m]$ , admet  $m$  pour unique point fixe. L'application  $g \mapsto \bar{g}$  induit donc un isomorphisme entre les normalisateurs  $N[M, m] \rightarrow N(M)$ . On a donc

$$N[M, m] = (g \in \mathcal{G} \mid g(m) = m \text{ et } \bar{g} \in N(M))$$

**3.3 Sections du groupe linéaire vers le groupe affine** . Soit  $A, B$  deux groupes de  $\mathcal{F}$ ,  $a, b$  deux points de  $\mathcal{E}$ . Si les couples  $(A, a)$  et  $(B, b)$  sont distincts, les groupes  $[A, a]$  et  $[B, b]$  sont distincts. L'application  $g \mapsto \bar{g}$  induit des isomorphismes  $N[A, a] \rightarrow N(A)$  et  $N[B, b] \rightarrow N(B)$ . Par ce qui précède, on a

$$N[A, a] \cap N[B, b] = (g \in \mathcal{G} \mid g(a) = a, g(b) = b, \bar{g} \in N(A) \cap N(B))$$

Si les couples  $(A, a)$  et  $(B, b)$  sont distincts,  $N[A, a] \cap N[B, b]$  n'est pas réduit à l'identité dans les trois cas suivants:

- $A = B$  et  $a \neq b$ : Soit  $\gamma$  l'unique rotation vectorielle d'ordre 3 reliée à  $A$  telle que  $\gamma(\vec{ab}) = \vec{ab}$  (Cf. 2.1, prop.3). Soit  $g \in \mathcal{G}$  tel que  $\bar{g} = \gamma$  et  $g(a) = a$ . Il est clair que  $\langle g \rangle = N[A, a] \cap N[B, b]$ .
- $A \neq B$  et  $a = b$ : Soit  $\gamma$  tel que  $\langle \gamma \rangle = N(A) \cap N(B)$  et  $g$  tel que  $\bar{g} = \gamma$  et  $g(a) = a$ . Il est clair que  $\langle g \rangle = N[A, a] \cap N[B, b]$ .
- Supposons  $A \neq B$  et  $a \neq b$ . Pour que  $g \in N[A, a] \cap N[B, b]$ , il faut et il suffit que  $g(a) = a$ ,  $g(b) = b$  et  $\bar{g} \in N(A) \cap N(B)$ . On pourra prendre  $g$  distincte de l'identité si et seulement si  $\vec{AB} = \vec{ab}$  au sens de la structure affine définie sur  $\mathcal{F}$  en 2.3.

Une première classe de sections est formées des  $s_a: f \mapsto f_a$  où  $a \in \mathcal{E}$ ,  $f_a$  étant l'application affine de point fixe  $a$  et d'application linéaire associée  $f$ .

Il existe 8 isomorphismes affines  $\mathcal{E} \rightarrow \mathcal{F}$  induisant l'identité sur l'espace  $E$  des vecteurs. Ils se déduisent les uns des autres par des translations. On détermine l'un d'eux  $\theta$  en fixant l'image  $A = \theta(a) \in \mathcal{F}$  d'un point  $a \in \mathcal{E}$ . Pour tout  $m \in \mathcal{E}$ ,  $M = \theta(m)$  est donné par  $\overrightarrow{AM} = \overrightarrow{am}$ . Considérons la section canonique (Cf.2.3) de  $G$  vers le groupe affine de  $\mathcal{F}$  associant à  $f \in G$  l'application affine

$$\tilde{f} : F \rightarrow \mathcal{F}, \mathcal{M} \mapsto f \mathcal{M} f^{-1}$$

L'application  $\sigma_\theta : f \mapsto \theta^{-1} \circ \tilde{f} \circ \theta$  constitue une section appartenant à une autre famille de 8 sections.

Réciproquement, soit une section  $s : G \rightarrow \mathcal{G}$ . Considérons deux sous-groupes  $A, B$  distincts de  $\mathcal{F}$ . Alors  $N(A) \cap N(B) = \langle \gamma \rangle$  où  $\gamma$  est d'ordre 3. On a  $s(A) = [A, a]$  et  $s(B) = [B, b]$  où  $(A, a)$  et  $(B, b)$  sont dans  $\mathcal{F} \times \mathcal{E}$ , ensemble des sous-groupes d'ordre 7 de  $\mathcal{G}$  et  $s(\gamma) = g \in N[Aaa] \cap N[B, b]$ . D'après ce qui précède, ou bien  $a = b$ , ou bien  $\overrightarrow{AB} = \overrightarrow{ab}$ .

Supposons que  $s$  n'est pas du type  $s_a$ . Il existe  $A, B$  dans  $\mathcal{F}$  tels que  $a \neq b$ . Soit alors  $M \in \mathcal{F}$  distincts de  $A$  et  $B$  et  $s(M) = [M, m]$ . Si on avait  $m = a$ , on aurait  $m \neq b$ , donc  $\overrightarrow{BM} = \overrightarrow{bm} = \overrightarrow{ba} = \overrightarrow{BA}$  ce qui est impossible car  $M \neq A$ . Ainsi,  $m$  est distinct de  $a, b$  et on a  $\overrightarrow{am} = \overrightarrow{AM}$  pour tout  $M \in \mathcal{F}$ .

La section  $s$  induit donc un isomorphisme  $\theta : \mathcal{E} \rightarrow \mathcal{F}, m \mapsto M$  induisant l'identité sur l'espace  $E$  des vecteurs. On voit alors que  $s = \sigma_\theta$  car  $s$  et  $\sigma_\theta$  concident en les éléments d'ordre 3 ou 7 qui engendrent le groupe  $G$ .

Les espaces affines isomorphes  $\mathcal{E}, \mathcal{F}, \mathcal{E}'$  ont même espace vectoriel  $E$ , donc même groupe linéaire  $G$  et même ensemble  $\mathcal{F}$ . Les espaces  $\mathcal{E}$  et  $\mathcal{E}'$  jouent le même rôle l'un par rapport à l'autre. En revanche, le groupe affine  $\mathcal{G}$  de  $\mathcal{E}$  et  $\mathcal{E}'$  ne s'identifie pas canoniquement au groupe affine de  $\mathcal{F}$ . Par exemple, on a 8 isomorphismes du groupe affine  $\mathcal{G}$  de  $\mathcal{E}$  sur le groupe affine de  $\mathcal{F}$  de la forme  $f \mapsto \theta f \theta^{-1}$  où  $\theta \in \mathcal{E}'$ .

### 3.4 L'ensemble $\mathcal{E}_1 = \mathcal{E} \cup \mathcal{E}'$ comme $\mathbf{F}_2$ -espace affine de dimension

4. Soit  $\mathcal{T}_1$  le groupe des automorphismes de  $\mathcal{G}$  induisant l'identité sur  $\mathcal{T}$  et sur  $G = \mathcal{G}/\mathcal{T}$ . À tout  $\vec{v} \in E$ , on associe l'automorphisme intérieur  $\hat{t}_{\vec{v}} : \varphi \mapsto t_{\vec{v}} \circ \varphi \circ t_{\vec{v}}$ . On a ainsi une inclusion  $t_{\vec{v}} \mapsto \hat{t}_{\vec{v}}$  de  $\mathcal{T}$  dans  $\mathcal{T}_1$ .

Soit  $s : G \hookrightarrow \mathcal{G}$  une section. On en déduit une bijection du produit ensembliste  $E \times G$  sur  $\mathcal{G}$ ,  $(\vec{v}, f) \mapsto t_{\vec{v}} \circ s(f)$ . Pour  $\vec{u}, \vec{v}$  dans  $E$  et  $f, g$

dans  $G$ , on a

$$\begin{aligned} t_{\vec{u}} \circ s(f) \circ t_{\vec{v}} \circ s(g) &= t_{\vec{u}} \circ \left( s(f) \circ t_{\vec{v}} \circ s(f^{-1}) \right) \circ s(f) \circ s(g) \\ &= t_{\vec{u}} \circ t_{f(\vec{v})} \circ s(fg) \end{aligned}$$

En transportant la structure de groupe de  $\mathcal{G}$  sur l'ensemble  $E \times G$  par cette bijection, on obtient la loi de groupe sur l'ensemble  $E \times G$

$$\left( \vec{u}, f \right) \left( \vec{v}, g \right) = \left( \vec{u} + f(\vec{v}), fg \right)$$

où l'image du sous-groupe  $(s(G))$  (resp.  $\mathcal{T}$ ) est le sous-groupe des  $(\vec{0}, f)$  (resp. le sous-groupe distingué des  $(\vec{v}, I_E)$ ).

Un automorphisme  $\Phi$  de  $\mathcal{G}$  induisant l'identité sur le sous-groupe  $\mathcal{T}$  et sur le quotient  $G = \mathcal{G}/\mathcal{T}$  se traduit par un automorphisme de  $E \times G$  de la forme

$$(\vec{v}, f) \mapsto (\vec{v} + \vec{\varphi}(f), f)$$

Le fait qu'il s'agit d'un automorphisme se traduit pour l'application  $\vec{\varphi} : G \rightarrow E$  par la propriété

$$\forall (f, g) \in G \times G, \quad \vec{\varphi}(fg) = f(\vec{\varphi}(g)) + \vec{\varphi}(f)$$

L'application  $\Phi \mapsto \vec{\varphi}$  est bijective de  $\mathcal{T}_1$  sur l'ensemble  $E_1$  des applications  $G \rightarrow E$  ayant cette propriété. La structure de  $\mathbf{F}_2$ -espace vectoriel de  $E$  induit une structure de  $\mathbf{F}_2$ -espace vectoriel sur  $E_1$ : l'addition de  $E_1$  est définie ainsi:

$$\forall (\vec{\varphi}, \vec{\psi}) \in E_1 \times E_1, \quad \forall f \in G, \quad \left( \vec{\varphi} + \vec{\psi} \right) (f) = \vec{\varphi}(f) + \vec{\psi}(f)$$

On vérifie aussi que la bijection  $\Phi \mapsto \vec{\varphi}$  de  $\mathcal{T}_1$  sur  $E_1$  est un isomorphisme de groupes, d'où la commutativité de  $\mathcal{T}_1$ . L'inclusion  $\mathcal{T} \hookrightarrow \mathcal{T}_1$  se traduit par une inclusion  $E \hookrightarrow E_1$ : au vecteur  $\vec{v}$  est associée l'application  $f \mapsto \vec{v} - f(\vec{v})$  de  $G$  vers  $E$ .

La commutativité de  $\mathcal{T}_1$  permet de voir que cet isomorphisme  $\mathcal{T} \rightarrow E_1$ ,  $\Phi \mapsto \vec{\varphi}$  est *canonique*, i.e. indépendant de la section  $s : G \hookrightarrow \mathcal{G}$  choisie pour le définir.

Le groupe  $\mathcal{T}_1$  opère simplement transitivement sur l'ensemble des sections  $\mathcal{E}_1 = \mathcal{E} \cup \mathcal{E}'$ : pour  $s \in \mathcal{E} \cup \mathcal{E}'$  et  $\Phi \in \mathcal{T}_1$ , on pose  $\Phi(s) = \Phi \circ s$ .

L'ensemble  $\mathcal{E}_1 = \mathcal{E} \cup \mathcal{E}'$  apparaît alors comme un  $\mathbf{F}_2$ -espace affine de dimension 4, d'espace vectoriel  $E_1$ , de groupe des translations  $\mathcal{T}_1$ ,  $\mathcal{E}$  et  $\mathcal{E}'$  étant les deux hyperplans parallèles de direction  $E$ .



Le quotient  $E_1/E \sim \mathcal{T}_1/\mathcal{T}$ , non trivial car de cardinal 2, est le premier groupe de cohomologie  $H_\psi^1(G, E)$ ,  $\psi$  étant l'isomorphisme  $G \rightarrow \text{Aut}(E)$  induit par l'opération de  $G$  sur  $E$ .

#### 4. $\mathbf{F}_2$ -espaces affines de dimensions supérieures

**4.1 Soit  $\mathcal{E}$  un  $\mathbf{F}_2$ -espace affine de dimension  $n \geq 4$ , de groupe affine  $\mathcal{G}$ , de groupe linéaire  $G$ , d'espace vectoriel associé  $E$ . Alors le cardinal de  $G$  est égal au nombre de bases, i.e.**

$$\begin{aligned} G &= (2^n - 1)(2^n - 2) \dots (2^n - 2^{n-1}) \\ &= (2^n - 1)(2^{n-1} - 1) \dots (2^2 - 1)2^{1+2+\dots+(n-1)} \\ &= (2^n - 1)(2^{n-1} - 1) \dots (2^2 - 1)2^{\frac{n(n-1)}{2}} \\ \mathcal{G} &= 2^n G = (2^n - 1)(2^{n-1} - 1) \dots (2^2 - 1)2^{\frac{n(n+1)}{2}} \end{aligned}$$

Supposons qu'il existe une section  $s : G \rightarrow \mathcal{G}$  non du type  $s_a$ . Montrons alors que  $s(G)$  agit transitivement sur  $\mathcal{E}$ .

Considérons l'extension  $\mathbf{F}_2 \hookrightarrow \mathbf{F}_{2^n}$ . Dans le groupe cyclique  $\mathbf{F}_{2^n}^\times$  existe un élément d'ordre  $2^n - 1$  de polynme minimal  $P(X)$  irréductible sur  $\mathbf{F}_2$  de degré  $n$ . Il existe donc dans  $G$  des applications d'ordre  $2^n - 1$  de polynme minimal  $P(X)$ . Comme 1 n'est pas valeur propre de  $f$ , tout relèvement de  $f$  dans  $\mathcal{G}$  a un unique point fixe dans  $\mathcal{E}$ . Il existe donc  $a \in \mathcal{E}$  tel que  $s(f) = f_a$  et les deux orbites du groupe cyclique  $\langle f_a \rangle$  sont  $\{a\}$  et  $\mathcal{E} \setminus \{a\}$ . Comme  $\{a\}$  n'est pas une orbite pour  $s(G)$ , l'action de  $s(G)$  est bien transitive.

**4.2 Cas  $n = 4$**  . On a dans  $G$  deux sortes d'applications d'ordre 3 selon que le polynme minimal est  $X^3 - 1$  ou  $X^2 + X + 1$ . On s'intéresse aux groupes cycliques du deuxième type. On raisonne dans l'espace projectif  $P = P(E)$  de dimension 3 et de cardinal  $16 - 1 = 15$ . Un tel groupe  $\gamma$  définit  $5 = \frac{15}{3}$  orbites sur  $P$  qui sont des droites disjointes.

On considère les triplets  $\gamma, D_1, D_2$  où  $D_1, D_2$  sont deux orbites de  $\gamma$ . La donnée de  $D_1, D_2$  et de deux permutations circulaires sur  $D_1, D_2$  détermine  $\gamma$ . deux droites disjointes  $D_1, D_2$  correspondent deux permutations circulaires sur chaque droite, donc deux groupes ayant  $D_1, D_2$  pour orbites.

L'ensemble des droites de  $P(E)$  est de cardinal  $\frac{1}{3}C_{15}^2 = \frac{14 \times 15}{6} = 35$ . L'ensemble des paires de droites est de cardinal  $C_{35}^2 = 17 \times 35$ . On a 15 plans projectifs dans  $P(E)$  et dans chacun d'eux 7 droites, donc  $C_7^2 = 21$  paires de droites. On a donc  $15 \times 21 = 9 \times 35$  paires de droites coplanaires. On a donc  $(17 - 9) \times 35 = 8 \times 35 = 280$  paires de droites disjointes. D'où

$280 \times 2 = 560$  triplets  $(\gamma, D_1, D_2) = (\gamma, D_2, D_1)$ . Pour chaque groupe  $\gamma$ , on a 5 orbites, donc  $C_5^2 = 10$  paires  $D_1, D_2$ . On en déduit que le nombre de groupes  $\gamma$  est  $\frac{560}{10} = 56$ .

Comme 1 n'est pas valeur propre de ces applications d'ordre 3, tout groupe  $\gamma$  se relève en un groupe  $\gamma_m$  où  $m \in \mathcal{E}$ . S'il existait une section  $s : G \rightarrow \mathcal{G}$  sans point fixe, les 16 stabilisateurs pour l'action de  $s(G)$  seraient tous conjugués. Comme 16 ne divise pas 56, il est impossible que les groupes  $\gamma$  se répartissent équitablement entre les 16 points de  $\mathcal{E}$ .

Ainsi, le théorème est démontré dans le cas  $n = 4$ . Ceci permet d'envisager une récurrence.

**4.3 Groupes de Klein de transvections** . Soit  $\vec{\varepsilon} \in E$  et  $u \in E^*$ , non nuls tels que  $u(\vec{\varepsilon}) = 0$ . La transvection vectorielle  $t_{\vec{\varepsilon}, u}$  est définie par

$$t_{\vec{\varepsilon}, u} : \vec{x} \mapsto \vec{x} + u(\vec{x}) \vec{\varepsilon}$$

Elle induit l'identité sur  $\ker u$  et la translation de vecteur  $\vec{\varepsilon}$  sur l'hyperplan affine des  $\vec{x}$  tels que  $u(\vec{x}) = 1$ . Elle est involutive.

On a deux classes de conjugaison de sous-groupes commutatifs de transvections de  $G$  de cardinal  $2^{n-1}$ :

- à  $u \in E^*$ , on associe  $T_u = \{t_{\vec{\varepsilon}, u} \mid \vec{\varepsilon} \in E \text{ et } u(\vec{\varepsilon}) = 0\}$
- à  $\vec{\varepsilon} \in E$ , on associe  $T_{\vec{\varepsilon}} = \{t_{\vec{\varepsilon}, u} \mid u \in E^* \text{ et } u(\vec{\varepsilon}) = 0\}$

On vérifie que :

$$\begin{aligned} \forall u \in E^*, \forall (\vec{\varepsilon}_1, \vec{\varepsilon}_2) \in E \times E, t_{\vec{\varepsilon}_1, u} \circ t_{\vec{\varepsilon}_2, u} &= t_{\vec{\varepsilon}_1 + \vec{\varepsilon}_2, u} \\ \forall \vec{\varepsilon} \in E, \forall (u_1, u_2) \in E^* \times E^*, t_{\vec{\varepsilon}, u_1} \circ t_{\vec{\varepsilon}, u_2} &= t_{\vec{\varepsilon}, u_1 + u_2} \end{aligned}$$

Les applications affines admettant la transvection vectorielle  $t_{\vec{\varepsilon}, u}$  pour application linéaire associée ne sont en général pas involutives. Celles qui le sont sont d'un des deux types suivants:

- les 2 transvections affines du type  $t_{\vec{\varepsilon}, A}$  induisant l'identité sur un hyperplan affine  $A$  de direction  $\ker u$  et la translation de vecteur  $\vec{\varepsilon}$  sur l'hyperplan parallèle,

- les  $2^{n-1} - 2$  relèvements affines involutifs sans points fixes  $t_{A, \vec{\alpha}; B, \vec{\beta}}$  où  $A$  et  $B$  sont les hyperplans de direction  $\ker u$  et  $\vec{\alpha} + \vec{\beta} = \vec{\varepsilon}$ , induisant sur les hyperplans affines  $A$  et  $B$  les translations de vecteurs  $\vec{\alpha}$  et  $\vec{\beta}$ .

On a deux types de groupes de Klein de transvections vectorielles:

$$K_{\vec{\varepsilon}, u, v, w} = \left\{ I_E, t_{\vec{\varepsilon}, u}, t_{\vec{\varepsilon}, v}, t_{\vec{\varepsilon}, w} \right\} \quad \text{où } u + v + w = 0$$

$$K_{\vec{\xi}, \vec{\eta}, \vec{\zeta}, u} = \left\{ I_E, t_{\vec{\xi}, u}, t_{\vec{\eta}, u}, t_{\vec{\zeta}, u} \right\} \quad \text{où } \vec{\xi} + \vec{\eta} + \vec{\zeta} = \vec{0}$$

**4.4 Lemme fondamental** . Soit  $u, v, w$  des formes linéaires distinctes vérifiant  $u + v + w = 0$ ,  $\vec{\varepsilon}$  un vecteur non nul,  $s : G \hookrightarrow \mathcal{G}$  une section,  $\Gamma = s \left( K_{\vec{\varepsilon}, u, v, w} \right)$ . Alors, si la dimension est  $n \geq 4$ , les éléments de  $\Gamma$  distincts de l'identité sont des transvections affines d'hyperplans concourants.

Le système de formes linéaires  $(u, v, w)$  se relève de 8 faons en un système de formes affines de somme constante sur  $\mathcal{E}$ . On note encore  $(u, v, w)$  un des 4 relèvements de formes affines de somme identiquement nulle sur  $\mathcal{E}$ . Considérons les 8 hyperplans affines

$$U_0 = \left\{ m \in \mathcal{E} \mid u(m) = 0 \right\} \quad , \quad U_1 = \left\{ m \in \mathcal{E} \mid u(m) = 1 \right\}$$

$$V_0 = \left\{ m \in \mathcal{E} \mid v(m) = 0 \right\} \quad , \quad V_1 = \left\{ m \in \mathcal{E} \mid v(m) = 1 \right\}$$

$$W_0 = \left\{ m \in \mathcal{E} \mid w(m) = 0 \right\} \quad , \quad W_1 = \left\{ m \in \mathcal{E} \mid w(m) = 1 \right\}$$

Supposons  $\Gamma$  formé des relèvements affines

$$t_u = t_{U_0, \vec{u}_0; U_1, \vec{u}_1} \quad , \quad t_v = t_{V_0, \vec{v}_0; V_1, \vec{v}_1} \quad , \quad t_w = t_{W_0, \vec{w}_0; W_1, \vec{w}_1}$$

$$\text{avec} \quad \begin{aligned} \vec{u}_0 + \vec{u}_1 &= \vec{\varepsilon} \text{ dans } \ker u \\ \vec{v}_0 + \vec{v}_1 &= \vec{\varepsilon} \text{ dans } \ker v \\ \vec{w}_0 + \vec{w}_1 &= \vec{\varepsilon} \text{ dans } \ker w \end{aligned}$$

On a les deux séries d'égalités

$$\begin{aligned}\vec{u}_0 + \vec{v}_0 + \vec{w}_0 &= \vec{u}_0 + \vec{v}_1 + \vec{w}_1 = \vec{u}_1 + \vec{v}_0 + \vec{w}_1 = \vec{u}_1 + \vec{v}_1 + \vec{w}_0 = \vec{\alpha} \\ \vec{u}_1 + \vec{v}_1 + \vec{w}_1 &= \vec{u}_1 + \vec{v}_0 + \vec{w}_0 = \vec{u}_0 + \vec{v}_1 + \vec{w}_0 = \vec{u}_0 + \vec{v}_0 + \vec{w}_1 = \vec{\beta}\end{aligned}$$

avec  $\vec{\alpha} + \vec{\beta} = \vec{\varepsilon}$ . L'hyperplan affine  $U_0 = (U_0 \cap V_0 \cap W_0) \cup (U_0 \cap V_1 \cap W_1)$  est stable par  $t_u$ .

- a) Supposons qu'il existe  $m \in U_0 \cap V_0 \cap W_0$  tel que  $t_u(m) = m + \vec{u}_0 \in U_0 \cap V_1 \cap W_1$ . Alors  $\vec{u}_0 \notin \ker v \cup \ker w$  et  $v(\vec{u}_0) = w(\vec{u}_0) = 1$ . On a

$$m + \vec{u}_0 + \vec{v}_1 = (t_v \circ t_u)(m) = t_w(m) = m + \vec{w}_0$$

donc  $\vec{\beta} = \vec{u}_0 + \vec{v}_1 + \vec{w}_0 = \vec{0}$  et  $\vec{\alpha} = \vec{\varepsilon}$ .

- b) Supposons qu'il existe  $m \in U_0 \cap V_0 \cap W_0$  tel que  $t_u(m) = m + \vec{u}_0 \in U_0 \cap V_0 \cap W_0$ . Alors  $\vec{u}_0 \in \ker u \cap \ker v \cap \ker w$  et  $v(\vec{u}_0) = w(\vec{u}_0) = 0$ . On a

$$m + \vec{u}_0 + \vec{v}_0 = (t_v \circ t_u)(m) = t_w(m) = m + \vec{w}_0$$

donc  $\vec{\alpha} = \vec{u}_0 + \vec{v}_0 + \vec{w}_0 = \vec{0}$  et  $\vec{\beta} = \vec{\varepsilon}$ .

Comme la dimension est  $n > 3$ ,  $\dim \ker u \geq 3$ . Il existe donc une forme linéaire non nulle  $v' \neq u$  telle que le plan vectoriel  $\{\vec{0}, \vec{\varepsilon}, \vec{u}_0, \vec{u}_1\}$  soit contenu dans  $\ker v'$ , donc aussi dans  $\ker w'$  où  $w' = u + v'$ . Le sous-groupe  $\Gamma = s(K_{\vec{\varepsilon}, u, v', w'})$  vérifie la condition b). Comme  $K_{\vec{\varepsilon}, u, v, w}$  est conjugué de  $K_{\vec{\varepsilon}, u, v', w'}$  dans  $G$ ,  $\Gamma' = s(K_{\vec{\varepsilon}, u, v', w'})$  et  $\Gamma = s(K_{\vec{\varepsilon}, u, v, w})$  sont conjugués dans  $s(G)$ . Ainsi,  $\Gamma$  vérifie la condition b).

Les sous-espaces affines  $U_0 \cap V_0 \cap W_0$  sont donc stables par  $t_u$ . En faisant varier les formes linéaires  $v$  et  $w$ , on voit finalement que les droites de  $U_0$  sont toutes stables par  $t_u$ , donc que  $\vec{u}_0 = \vec{\varepsilon}$ ,  $\vec{u}_1 = \vec{0}$ , d'où  $t_u$  est la transvection affine d'hyperplan  $U_0$  de vecteur  $\vec{\varepsilon}$ .

Comme toute transvection vectorielle appartient à un groupe du type  $K_{\vec{\varepsilon}, u, v, w}$ , on déduit du lemme le corollaire ci-dessous:

**Corollaire** *L'image d'une transvection vectorielle par une section  $s : G \hookrightarrow \mathcal{G}$  est une transvection affine.*

Dans la suite, pour montrer le théorème, on suppose la dimension  $n \geq 5$ , l'hypothèse de récurrence étant que le théorème est supposé vrai en dimension  $n - 1$ . On donne une section  $s : G \hookrightarrow \mathcal{G}$ . Il s'agit de montrer qu'elle est du type  $s_a$  où  $a \in \mathcal{E}$ .

**4.5 Le groupe  $S_u$  où  $u \in E^*$**  . Soit  $u \in E^*$  un forme linéaire non nulle. On forme le sous-groupe de  $G$

$$S_u = \{f \in G \mid u \circ f = u\}$$

Alors  $S_u$  opère sur les hyperplans stables vectoriel et affine

$$F_{u,0} = \ker u = \{\vec{x} \in E \mid u(\vec{x}) = 0\}, \quad F_{u,1} = \{\vec{x} \in E \mid u(\vec{x}) = 1\}$$

L'action de  $S_u$  sur  $F_{u,1}$  permet d'identifier  $S_u$  au groupe affine. Alors  $F_{u,0}$  s'identifie à l'espace des vecteurs de  $F_{u,1}$ . L'application  $S_u \rightarrow F_{u,0}$  associant à  $f \in S_u$  sa restriction à  $F_{u,0}$  est la surjection canonique du groupe affine sur le groupe linéaire. Le noyau  $T_u$ , groupe des transvections d'hyperplan  $F_{u,0}$ , s'identifie au groupe des translations de l'espace affine  $F_{u,1}$ , la transvection  $t_{\vec{\varepsilon},u}$  s'identifiant à la translation de vecteur  $\vec{\varepsilon}$ .

L'hypothèse de récurrence permet d'affirmer que les sections  $GL(F_{u,0}) \hookrightarrow S_u$  envoient  $GL(F_{u,0})$  en des sous-groupes de  $S_u$  de la forme

$$G_{\vec{\delta},u} = \{f \in S_u \mid f(\vec{\delta}) = \vec{\delta}\} = \{f \in G \mid f(\vec{\delta}) = \vec{\delta} \text{ et } u \circ f = u\}$$

Soit  $A, B$  les deux hyperplans de  $\mathcal{E}$  de direction  $F_{u,0}$ .

Pour qu'une application affine ait son application linéaire associée dans  $S_u$ , il faut et il suffit que les hyperplans  $A$  et  $B$ , ou bien soient stables, ou bien soient échangés. Ces applications affines forment un sous-groupe  $\mathcal{K}_\square$  admettant pour sous-groupe d'indice 2 le sous-groupe  $\mathcal{H}_\square$  des applications affines laissant  $A$  et  $B$  stables.

Montrons que  $S_u$  n'a pas de sous-groupes d'indice 2. Comme les groupes linéaires sont simples en dimension au moins 3, les  $G_{\vec{\delta},u}$  sont contenus dans tout sous-groupe d'indice 2 de  $S_u$ . Il suffit de montrer que  $S_u$  est engendré par les sous-groupes  $G_{\vec{\delta},u}$ .

Soit  $\vec{\varepsilon} \in F_{u,0}$ ,  $\vec{\delta} \notin F_{u,0}$ ,  $\vec{\delta}_1 = \vec{\delta} + \vec{\varepsilon}$ . Soit  $f \in G_{\vec{\delta},u}$  et  $f_1 \in G_{\vec{\delta}_1,u}$  de même application linéaire associée  $g$ . Alors  $f_1 \circ f^{-1}$  envoie  $\vec{\delta}$  en  $g(\vec{\delta}) + \vec{\varepsilon}$  donc est la transvection de vecteur  $g(\vec{\delta}) + \vec{\delta} + \vec{\varepsilon}$ . Comme  $g(\vec{\delta})$  peut être pris quelconque dans  $F_{u,1}$ , toute transvection est dans le sous-groupe engendré par les  $G_{\vec{\delta},u}$ .

La section  $s$  envoie donc  $S_u$  dans le sous-groupe  $\mathcal{H}_\square$  des applications affines laissant les hyperplans parallèles  $A$  et  $B$  stables. Soit  $\mathcal{A}$  et  $\mathcal{B}$  les groupes affines de  $A$  et  $B$ . En prenant les restrictions à  $A$  et  $B$  des  $s(f)$

où  $f \in S_u$ , on a des morphismes  $S_u \rightarrow \mathcal{A}$  et  $S_u \rightarrow \mathcal{B}$  dont les noyaux ne sont formés que de transvections. Pour tout  $\vec{\delta} \in F_{u,1}$ , les restrictions de ces morphismes à  $G_{\vec{\delta},u}$  donnent des morphismes injectifs  $G_{\vec{\delta},u} \hookrightarrow \mathcal{A}$  et  $G_{\vec{\delta},u} \hookrightarrow \mathcal{B}$  qu'on peut considérer comme des sections du groupe linéaire dans le groupe affine en dimension  $n-1$ . L'hypothèse de récurrence permet d'affirmer qu'il existe  $a \in A$  et  $b \in B$  fixes par tout  $s(g)$  où  $g \in G_{\vec{\delta},u}$ .

Ainsi, pour toute section  $s : G \hookrightarrow \mathcal{G}$  et tout sous-groupe  $G_{\vec{\delta},u} \subset G$ , il existe  $a \in A$  et  $b \in B$  tels que  $\vec{ab} = \vec{\delta}$  et que  $s(G_{\vec{\delta},u})$  soit le sous-groupe  $G_{a,b,u} \subset \mathcal{G}$  des applications affines de  $\mathcal{E}$  laissant fixes les points  $a$  et  $b$ , stables les hyperplans  $A = a + F_{u,0}$  et  $B = b + F_{u,0}$ .

**4.6 Lemme** Soit  $s : G \hookrightarrow \mathcal{G}$  une section et  $u \in E^*$  une forme linéaire non nulle. Il existe un unique point  $a \in \mathcal{E}$  fixe pour toutes les applications de  $s(S_u)$ .

Soit  $\vec{\varepsilon}_1$  dans  $F_{u,0}$ ,  $\vec{\delta}$  et  $\vec{\delta}_1 = \vec{\delta} + \vec{\varepsilon}_1$  dans  $F_{u,1}$ , on a  $G_{\vec{\delta}_1,u} = t_{\vec{\varepsilon}_1,u} G_{\vec{\delta},u} t_{\vec{\varepsilon}_1,u}$ . Par 4.4,  $s(t_{\vec{\varepsilon}_1,u})$  est une transvection de vecteur  $\vec{\varepsilon}_1$  et d'hyperplan  $A$  ou  $B$ . Posant  $s(G_{\vec{\delta},u}) = G_{a,b,u}$  et  $s(G_{\vec{\delta}_1,u}) = G_{a_1,b_1,u}$ , par conjugaison, la transvection affine  $s(t_{\vec{\varepsilon}_1,u})$  envoie  $a$  et  $b$  en  $a_1$  et  $b_1$ . On a donc ou bien  $a_1 = a$  et  $b_1 = b + \vec{\varepsilon}_1$ , ou bien  $a_1 = a + \vec{\varepsilon}_1$  et  $b_1 = b$ .

Soit  $\vec{\varepsilon}_2 \neq \vec{\varepsilon}_1$  dans  $F_{u,0}$  et  $\vec{\delta}_2 = \vec{\delta}_1 + \vec{\varepsilon}_2$ ,  $s(G_{\vec{\delta}_2,u}) = G_{a_2,b_2,u}$ . Supposons  $\vec{bb}_1 = \vec{\varepsilon}_1$ . Alors  $\vec{bb}_2 = \vec{bb}_1 + \vec{b}_1\vec{b}_2 = \vec{\varepsilon}_1 + \vec{b}_1\vec{b}_2$  est égal à  $\vec{0}$  ou  $\vec{\varepsilon}_1 + \vec{\varepsilon}_2$ . Comme  $\vec{b}_1\vec{b}_2$  vaut  $\vec{0}$  ou  $\vec{\varepsilon}_2$ , la seule possibilité est  $\vec{b}_1\vec{b}_2 = \vec{\varepsilon}_2$  et  $\vec{bb}_2 = \vec{\varepsilon}_1 + \vec{\varepsilon}_2$ . On a alors  $a = a_1 = a_2$ . Les groupes  $s(G_{\vec{\delta},u})$  sont donc tous de la forme  $G_{a,b,u}$  où  $a \in A$  est indépendant de  $\vec{\delta}$ . Comme les  $s(G_{\vec{\delta},u})$  engendrent  $s(S_u)$ ,  $a$  est bien point fixe de toutes les applications de  $s(S_u)$ .

On obtient l'unicité de  $a$  ainsi. Soit  $\vec{\delta}$  et  $\vec{\delta}_1$  distincts dans  $F_{u,1}$ ,  $f \in G_{\vec{\delta},u}$  (resp.  $f_1 \in G_{\vec{\delta}_1,u}$ ) admettant  $\vec{\delta}$  (resp.  $\vec{\delta}_1$ ) pour unique vecteur fixe. Alors  $s(f)$  (resp.  $s(f_1)$ ) admet  $a$  et  $b = a + \vec{\delta}$  (resp.  $a$  et  $b_1 = a + \vec{\delta}_1$ ) pour seuls points fixes. Comme  $b \neq b_1$ ,  $a$  est l'unique point fixe commun aux  $s(g)$  où  $g$  décrit  $S_u$ . Ce point  $a$  dépendant à priori de  $u$ , on le note  $a_u$ .

**4.7 Fin de la preuve** Supposons que la section  $s : G \hookrightarrow \mathcal{G}$  ne soit pas du type  $s_a$ . Par 4.1, l'action de  $s(G)$  sur  $\mathcal{E}$  serait transitive. Tout point de  $\mathcal{E}$  serait d'au moins une façon de la forme  $a_u$  où  $u \in E^*$ ,  $u \neq 0$ . C'est impossible car il n'existe que  $2^n - 1$  formes linéaires non nulles et  $2^n$  points dans  $\mathcal{E}$ .

### References

- [1] Arnaudiès J. M., Bertin J. *Groupes, Algèbres et Géométrie*, Ellipses, (1993).
- [2] Coxeter H. S. M., *Introduction to geometry* (J. Wiley and Sons, (1989).
- [3] Dieudonné J., *Algèbre linéaire et géométrie élémentaire*, Hermann, (1968).
- [4] Hilbert D. et Cohn-Vossen S. *Geometry and the imagination*, Chelsea, (1952).
- [5] Mac Lane S. *Homology*, Springer-Verlage, (1963).
- [6] Perrin D., *Cours d'algèbre*, Ellipses, (1996).
- [7] Samuel P., *Géométrie projective*, PUF, (1986).

### Remi Goblot

UFR de Mathématiques  
Université de Lille I  
59655 Villeneuve D'Ascq Cedex  
France  
e-mail : goblot@math.univ-lille1.fr