Géométrie projective abstraite et algèbres d'octonions

Alexander Semenov, Ludovic Schwartz
sous la directtion de Cyril Demarche

30 juin 2016

Résumé

Les espaces projectifs à coordonnées définies sur un corps sont fort connus et vérfient un certain nombre de propriétés. Néanmoins, ce n'est pas la seule façon de définir un plan projectif. On peut aussi les voir comme un ensemble de points et de droites qui vérifient un certain nombre d'axiomes (approche d'Euclide). Les axiomes qu'on impose alors sont vérifiés par les plans projectifs issus de l'algèbre linéaire. Néanmoins, les plans issus de l'algèbre linéaire ne sont pas nécessairement les seuls à vérifier les axiomes qu'on fixe. On verra d'abord qu'il existe un système d'axiomes qui redonne exactement les plans projectifs habituels. On verra aussi qu'on obtient des plans projectifs avec une certaine régularité lorsqu'on affaiblit (mais pas trop) les axiomes. On découvrira une corrélation entre les propriétés géométriques du plan et les propriétés algébriques de l'ensemble des coordonnées. Ceci nous donnera l'occasion de découvrir des plans projectifs à coordonnées dans un objet un peu moins régulier qu'un corps et de mettre le jour sur les algèbres d'octonions. On verra enfin qu'il existe très peu de plans finis exotiques dans un sens qu'on verra. On obtiendra un début de classification des plans projectifs axiomatiques, plus précisément on aura une classification claire de plans projectifs axiomatiques suffisamment réguliers.

Première partie

Plans projectifs habituels et axiomes qui suffisent pour les retrouver

1 Les plans projectifs habituels

Soit K est un anneau à division (i.e. un corps qu'on ne suppose pas commutatif). On remarque que les bases des espaces vectoriels sur K ont les mêmes propriétés que lorsque K est commutatif (c'est-à-dire que les bases de K^3 ont toutes trois éléments, et les plans vectoriels de K^3 sont engendrés par n'importe quelle paire de vecteurs linéairement indépendants qu'ils contiennent).

Définition K^* agit sur K^3 par multiplication à gauche $\lambda.(x_1, x_2, x_3) = (\lambda x_1, \lambda x_2, \lambda x_3)$

On pose $P_2(K) = K^3/K^*$

On peut le voir comme l'ensemble des droites vectorielles de K^3.

Les droites (projectives) de $P_2(K)$ sont définis comme les images des plans vectoriels de K^3 par l'application quotient.

Coordonnées Chaque point de $P_2(K)$ est repéré par ses **coordonnées homogènes**, c'est-à-dire par $(x : y : z)$ où $x, y, z \in K$ et ne sont pas tous les trois nuls. Les coordonnées homogènes sont définis à multiplication à gauche par un scalaire non nul près. Ils correspondent aux coordonnées de n'importe quel point de l'image réciproque par l'application quotient du point considéré du plan projectif.

Forme linéaire sur K^3 Il faut faire attention lorsqu'on travaille avec des corps non commutatifs, d'où la nécessité de ce paragraphe. Toute forme linéaire non nulle sur K^3 est de la forme $(x, y, z) \longmapsto xa + yb + zc$ où $(a, b, c) \neq (0, 0, 0)$. Le noyau d'une forme linéaire est un plan vectoriel. Et pour tout plan, les coordonnées (a, b, c) de la forme linéaire qui l'annulent existent et sont définis à multiplication à droite par un scalaire non nul près.

Plan dual Ainsi, l'ensemble des droites de $P_2(K)$ s'identifie à un plan projectif sur K.

2 Ce qu'on demande à n'importe quel objet qui pourrait s'appeler plan

2.1 Définition

Un plan Π est un couple (P, D) où P est un ensemble de «points » de cardinal au moins 3 et D est un ensemble de cardinal au moins 3 de parties à au moins deux éléments de P, dont les éléments sont appelés «droites ».

Les restrictions au niveau de la cardinalité des deux ensembles sont raisonnables car on veut exclure le cas de plans réduits à une seule droite.

2.2 Axiomes

On veut pouvoir pouvoir définir une droite par deux points distincts du plan, c'est-à-dire parler de la droite (AB).

Axiome 1 (P1) Par deux points distincts, il passe une droite et une seule.

Ainsi, on demande tout simplement le fait suivant : l'ensemble des paires de points se surjecte dans l'ensemble des droites par l'application qui à une paire de points donne l'unique droite qui passe par cette paire de points. On appelera cette application **incidence**.

Cet axiome est ce qu'il y a de plus minimal pour qu'un couple (P, D) puisse s'appeler plan.

Remarque Dans ce sens, $P_2(K)$ est un plan.

3 Plan projectif général

L'axiome (P1) donne un objet trop général. On énoncera les axiomes pour mettre en oeuvre un concept de base supplémentaire qu'auront tous les plans qu'on étudiera : la dualité.

3.1 Dualité

Cela consiste à pouvoir interchanger les notions de point et de droite. Soit Π un plan. On notera Π^* son plan dual. Les points de Π^* sont alors les droites de Π et les droites de Π^* sont les points de Π. Expliquons comment c'est possible.

Si d est une droite de Π, elle est définie comme l'ensemble des points qui appartiennent à d. On dira qu'un point A et qu'une droite a sont **incidents** lorsque $A \in a$. Ainsi, une droite d de Π est l'ensemble des points de Π incidents à d.

Renversons la situation. On appelera **droite duale** de Π définie par un point A comme l'ensemble des droites de Π incidentes au point A.

Les droites duales de Π sont donc en correspondance bijective avec les points de Π.

Ainsi, si Π est un plan tel que les droites duales sont toutes des ensembles à au moins deux éléments, on définit :

Définition Le plan dual Π^* de Π est un plan tel que ses points sont les droites de Π et ses droites sont les droites duales de Π.

On remarque immédiatement que le dual du dual s'identifie au plan de départ (cette identification préserve toutes les relations d'incidence).

Étant donné un énoncé relatif à un plan donné, on appelera énoncé dual, le même énoncé relatif à son plan dual.

3.2 Axiomes

Si Π est un plan au sens de l'axiome (P1), on aimerait que Π^* le soit aussi. Cela revient à demander que l'ensemble des paires de droites se surjecte dans l'ensemble des points, c'est-à-dire l'axiome suivant qui est le dual de (P1) :

Axiome 2 (P2) Deux droites distinctes se coupent en un point et un seul.

Il est aussi nécessaire de vérifier que par chaque point il passe au moins deux droites. Pour cela, il suffit qu'il existe un triangle (c'est-à-dire trois points non alignés). Remarquons que cet énoncé est équivalent à son dual modulo (P1) et (P2) : il existe un trilatère (c'est-à-dire trois droites non concourantes). Il suffit de choisir deux droites distinctes d_1 et d_2, de prendre A leur point d'intersection et de choisir B et C deuxièmes points respectivement sur d_1 et sur d_2. A, B, C sont alors non alignés.

On appelera **plan projectif général** un plan qui vérifie (P1) et (P2). On rajoutera encore des axiomes à cette liste un peu plus loin.

Remarque $P_2(K)$ est donc un plan projectif général.

3.3 Insatisfaction

À première vue, l'objet qu'on a défini ne semble même pas décrire le plan de la vie réelle, car n'a pas de droites parallèles et que peut-être avoir la dualité était de trop... On verra un peu plus loin qu'on n'a rien perdu et que la dualité vient naturellement.

3.4 Exemples et axiomes supplémentaires

3.4.1 Axiome du quadrangle

On a déjà vu que tout plan projectif général possède un triangle (c'est-à-dire trois points non colinéaires). Mais, il n'est pas certifié qu'un plan projectif général possède un quadrangle (quatre points, trois à trois non alignés). Dans la suite, nous nous intéresserons seulement aux plans projectifs généraux vérifiant l'axiome supplémentaire suivant :

Axiome du quadrangle (P3) Il existe un quadrangle (quatre points, trois à trois non alignés).

On remarque que (P3) est équivalent à son dual (axiome du quadrilatère) modulo les axiomes (P1) et (P2)

Remarque Cette axiome est vérifié dans $P_2(K)$: il suffit de prendre les points $(1:0:0)$, $(0:1:0)$, $(0:0:1)$ et $(1:1:1)$.

3.4.2 Plan projectif général

On appelera désormais plan projectif général tout plan vérifiant les axiomes (P1), (P2) et (P3).

3.4.3 Liste des plans vérifiant (P1), (P2), non-(P3)

On les appelle les plans dégénerés.

Le triangle Plan constitué de trois points non alignés et des droites joignant ces trois points (trois points et trois droites)

Le triangle enrichi On peut dans le plan précédemment défini choisir une droite et rajouter autant de points qu'on veut dessus, ainsi que les droites qui joignent les points rajoutés au point qui n'est pas sur la droite.

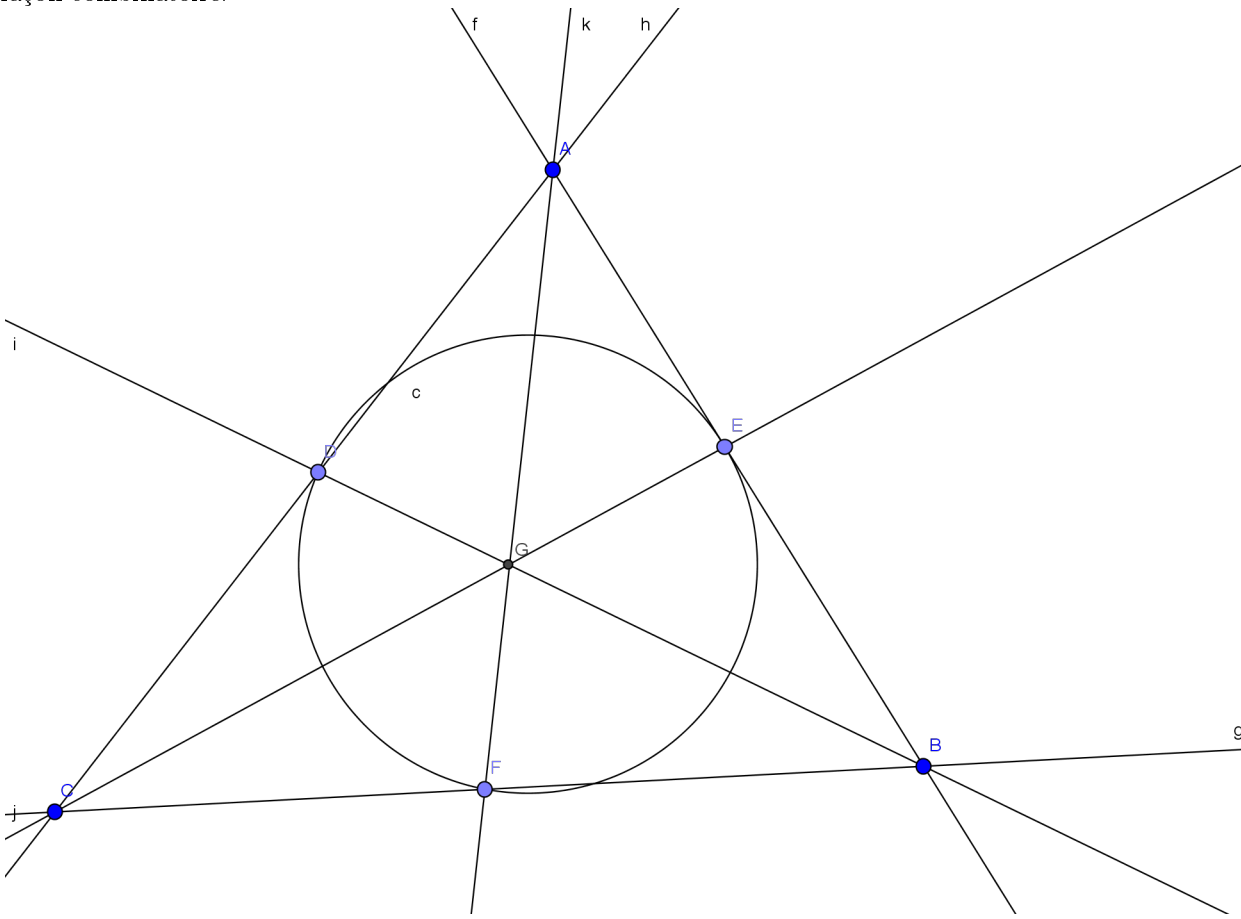
Rien d'autre On a déjà remarqué qu'il existe toujours trois points formant un triangle. On a décrit ci-dessus où peuvent se trouver les autres points et les droites pour que le plan vérifie non-(P3). Remarquons déjà que dès qu'il existe un point extérieur aux droites formant le triangle, le plan vérifie (P3). Puis, on remarque facilement que dès qu'il existe des points supplémentaires sur deux des droites formant le triangle, on trouve facilement un point extérieur aux droites formant le triangle.

On remarque aussi que (P3) est équivalent au fait que pour tout triangle on peut trouver un quatrième point de sorte à obtenir un quadrangle.

On en déduit que pour un plan projectif vérifiant (P1), (P2) et (P3), toute droite contient au moins trois points. De plus, toute droite contient le même nombre de points. On voit aussi qu'une droite duale a le même nombre de points qu'une droite. Et si chaque droite contient $q+1$ points, alors le nombre total de points du plan est $q(q+1)+1 = q^2+q+1$, c'est aussi le nombre total de droites. q peut prendre des valeurs a priori quelconques, mais dans le cas des plans projectifs usuels finis, q est une puissance d'un nombre premier.

En fait, les plans projectifs vérifiant (P1), (P2) et (P3) apparaiteront naturellement à partir des «plans de la vie réelle ».

Remarque Le plus petit des plans usuels (c'est-à-dire celui qui a le moins de points) est $P_2(F_2)$, le plan de Fano, qui a 7 points et 7 droites. C'est d'ailleurs aussi le plus petit plan vérifiant les axiomes donnés ci-dessus. On peut le vérifier de façon combinatoire.



4 Plan affine

Le but est de remarquer que les plans affines ne donnent pas d'objets vraiment nouveaux par rapport aux plans projectifs. Leur étude se ramène donc à l'étude des plans projectifs.

4.1 Axiomes

Donnons les axiomes les plus fondamentaux que vérifie le plan de la vie réelle. Dans notre cadre d'étude, on appelera **plan affine général** un plan vérifiant les axiomes ci-dessous. On demande déjà l'axiome (P1) qu'on appelera ici (A1). On dira que deux droites l et m sont parallèles lorsque soit $l = m$ soit l et m

n'ont aucun point en commun. On remarque que (A1) implique que deux droites distinctes ont au plus un point d'intersection. On peut dire : deux droites non parallèles ont un point d'intersection et un seul.

Axiome 2 (A2) Pour un point P et une droite l donnés, il existe une unique droite m parallèle à l et passant par P.

On en déduit que le parallélisme entre droites est une relation d'équivalence.

Dans un plan projectif, si on choisit une droite et un point extérieur à cette droite, on a une bijection par incidence entre la droite et la droite duale. Ce que cet axiome raconte c'est que dans un plan affine c'est pareil si on prive la droite duale de la droite parallèle à la droite considérée.

On remarque aisément que dans tout plan affine il existe un triangle (c'est-à-dire trois points non alignés).

4.2 Plan affine réalisé dans le plan projectif

Donnons-nous un plan projectif, et choisissons une droite d_∞ qu'on appelera «droite à l'infini ». Enlevons cette droite à l'ensemble des droites et tous les points incidents à cette droite à l'ensemble des points. Les droites sont alors les anciennes droites auxquelles on a enlevé le point d'intersection avec d_∞. L'ensemble des nouvelles droites est en bijection avec l'ensemble des anciennes droites privé de d_∞. Assurons-nous qu'on obtient ainsi un plan affine. On a toujours un plan, car il y a toujours au moins trois points, au moins trois droites et chaque droite possède au moins deux points. Lorsqu'on a deux points A et B, la droite (AB) n'est pas d_∞ donc (A1) est vérifié. (A2) est vérifié, car deux droites sont parallèles SSI leur point d'intersection se trouvait sur d_∞.

4.3 Plan projectif comme complétion d'un plan affine

Donnons nous un plan affine. Remplaçons l'ensemble des points par la réunion disjointe de l'ensemble des points initial (les points «à distance finie ») et de l'ensemble des classes d'équivalence des droites parallèles (les points «à l'infini »). À chaque droite, on rajoute le point correspondant à la classe d'équivalence dont la droite en question fait partie, qu'on appelera «point à l'infini » de la droite. On rajoute enfin à l'ensemble des droite une «droite à l'infini » d_∞ dont les éléments sont les classes d'équivalence de droites parallèles. Étant donné que dans un plan affine il existe un triangle, d_∞ contient au moins trois points. Toute autre droite, aussi, contient au moins trois points : au moins deux points «à distance finie » et un point «à l'infini ».

Le plan obtenu vérifie (P1). C'est une conséquence de (A1) si on prend deux points à distance finie. C'est une conséquence de (A2) si on prend un point à distance finie et un point à l'infini. C'est vrai par définition de d_∞ si on prend deux points à l'infini.

Le plan obtenu vérifie (P2). Si on prend deux droites différentes de d_∞, si elles ne sont pas parallèles leur point d'intersection correspond à leur point

d'intersection dans le plan affine initial, si elles sont parallèles leur point d'intersection correspond à leur classe d'équivalence. Si on prend une droite et d_∞, le point d'intersection est le point à l'infini.

Le plan obtenu vérifie (P3). On peut déjà prendre un triangle ABC constitué de points à distance finie. Ensuite, on prend la droite d passant par A et parallèle à (BC). Et on prend sur d un deuxième point à distance finie D. Alors $ABCD$ est le quadrangle dont on a besoin.

4.4 Conclusion

L'étude des plans affines revient à l'étude des plans projectifs dont on a choisi une droite à l'infini. D'où le choix de travailler dans des plans projectifs uniquement.

5 Isomorphisme entre deux plans projectifs généraux

On dira que deux plans projectifs généraux E et F sont isomorphes lorsqu'il existe une bijection entre leurs ensembles de points f et une bijection entre leurs ensembles de droites g telles que $A \in E$ est incident à $d \in E*$ si et seulement si $f(A)$ est incident à $g(d)$.

Il est clair que g est entièrement déterminée par f et réciproquement. On peut donc de façon équivalente demander que f soit une bijection et que A, B, C sont alignés SSI $f(A), f(B), f(C)$ sont alignés (sans parler de g).

Les automorphismes d'un plan projectif général donné forment bien entendu un groupe.

On appelera **collinéation** un isomorphisme ainsi défini.

Question Est-ce qu'un plan projectif général est toujours isomorphe à son dual ?

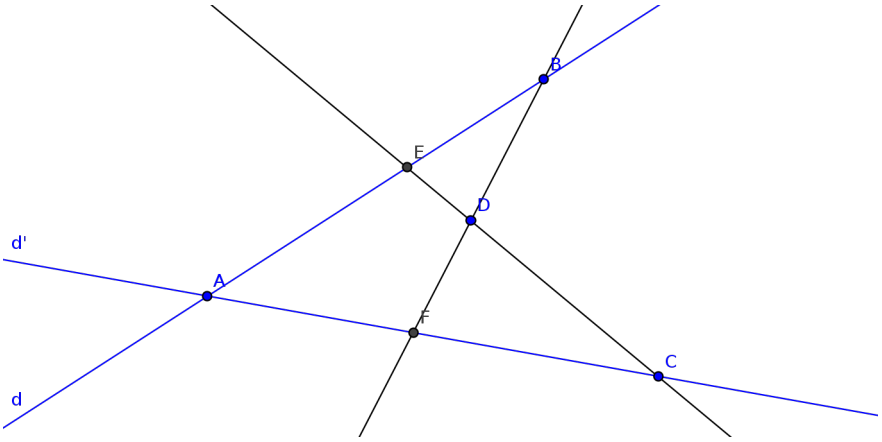
On n'a pas su répondre à cette question.

5.1 Collinéations particulières : les perspectives

On va s'intéresser aux éléments du groupe des automorphismes d'un plan projectif général Π.

Propriété Soit f une autocollinéation qui fixe les points de deux droites d et d'. Alors f est l'identité.

Preuve On montre que tout point est fixe selon le schéma suivant :



On montre que le point D est fixe.

Définition Une autocollinéation différente de l'identité est dite **perspective** s'il existe une droite d dont elle fixe les points. Cette droite est dite **axe de la perspective**.

Remarque Une droite qui joint un point (non fixe) avec son image par une perspective est fixe par cette perspective.

Remarque Si O est un point fixe extérieur à d alors toute droite passant par O est fixe.

Remarque Toutes les droites fixes différentes de d sont concourantes. Il existe une droite fixe différente de d.

Théorème Une perspective f (d'axe d) réalise aussi une perspective sur le plan dual.

Preuve Il suffit de montrer qu'il existe un point O, qui sera appelé **centre de la perspective**, telle que f fixe toutes les droites passant par O (ATTENTION : pas les points des droites, les points sur une droite passant par O peuvent bouger mais en restant sur la droite).

Soit A un point extérieur à la droite d.

1) Si A n'est pas fixe, alors $(Af(A))$ est fixe. Mais il existe un point B extérieur à d et à $(Af(A))$. B n'est pas fixe, car sinon toute droite passant par B est fixe, et en intersectant avec $(Af(A))$, tout point de $(Af(A))$ est fixe et donc f est identité, contradiction. $(Bf(B))$ est une droite différente de $(Af(A))$ et est fixe. Soit $O = (Af(A)) \cap (Bf(B))$. Alors O est le point voulu.

2) Si A est fixe. $O = A$ est le point voulu.

Remarque On appelle **translation** une perspective dont le centre se trouve sur l'axe. Elles sont appelées **élations** dans certaines référnces. Elle n'a pas de points fixes ailleurs que sur l'axe. On peut alors voir l'axe comme la droite à l'infini et le centre comme la direction de la translation.

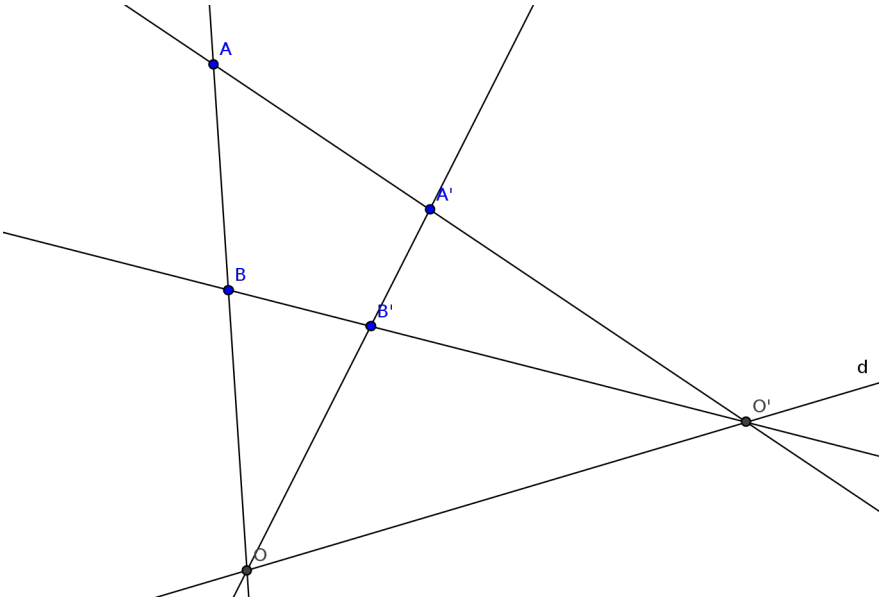
Les perspectives qui ne sont pas des translations peuvent être vues comme des homothéties si on choisit toujours l'axe pour droite à l'infini. Elles sont appelées **homologies**.

On peut vérifier qu'on obtient exactement ces transformations là avec les plans projectifs usuels (c'est-à-dire sur un corps).

Remarque L'existence des perspectives pour un plan projectif général donné est l'objet de la partie suivante. On peut remarquer que l'énoncé d'existence d'une perspective est équivalent à son énoncé dual modulo les axiomes d'un plan projectif général. On peut aussi remarquer que l'existence d'une perspective d'axe d et de centre O pour tous d et O est vérifiée dans un $P_2(K)$. Si on définit un espace tridimensionnel projectif muni des seules axiomes d'incidence, analogues à celles données ci-dessus pour un plan, on vérifie aisément l'existence d'une perspective d'axe d et de centre O pour tous d et O. Ainsi, les plans exotiques avec lesquels on fera connaissance dans la partie suivante ne peuvent pas vivre dans un espace projectif tridimensionnel.

Remarque L'ensemble des perspectives réuni avec l'identité ne forme pas en général un sous-groupe du groupe des autocollinéations.

Toutefois, si on choisit une droite d. L'ensemble des perspectives d'axe d réuni avec l'identité forme un sous-groupe du groupe des autocollinéations : le groupe des perspectives d'axe d. L'ensemble des translations d'axe d est un sous-groupe du groupe des perspectives d'axe d : le groupe des translations d'axe d (preuve facile : il faut faire une petite construction). Dans ce document, on supposera toujours que pour toute droite d, le groupe des translations d'axe d agit transitivement sur les points extérieurs à d. Sous cette hypothèse, on vérifie que ce dernier groupe est abélien. La figure suivante montre que deux translations de centres différents communtent :



Pour montrer que deux translations de même centre commutent, il suffit d'écrire l'une des deux comme composée de deux translations de centres différents.

Pourquoi les perspectives ? Il s'agit, en un certain sens, des collinéations les plus simples. Il y a trois façon de le comprendre :

- Elles s'obtiennent à partir des premières collinéations auquelles on pense : les projections centrales d'un plan sur un autre plongés dans un espace tridimensionnel
- C'est les seules collinéations qui ont un sens affine : on peut considérer la droite qu'on fixe comme la droite à l'infini. Ainsi, on considère les collinéations qui agissent sur les points « à distance finie » d'un plan affine obtenu en choisissant une droite à l'infini quelconque et qui préservent les directions des droites
- Dans le cas d'un plan projectif standard (sur corps), c'est des collinéations qui ont une expression matricielle particulièrement simple dans une base bien choisie, à savoir elle sont sous la forme $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \alpha \end{pmatrix}$.

6 Propriétés vraies

6.1 Théorème de Désargues

Le théorème de Desargues est vrai dans $P_2(K)$.

Enoncé (affine) Soient ABC et A'B'C' deux triangles dans le plan affine, sans sommets communs et tels que (AB)//(A'B') , (BC)//(B'C') , (CA)//(C'A') Alors les droites (AA'), (BB') et (CC') sont parallèles ou concourantes.

Preuve Ce résultat se déduit du théorème de Thalès et de sa réciproque.

Enoncé(projectif) Soient ABC et A'B'C' deux triangles dans l'espace projectif, sans sommets communs et tels que les droites (AA'), (BB'), (CC') soient distinctes. On note : P = (BC)∩(B'C') , Q = (CA)∩(C'A') , R = (AB)∩(A'B') Alors P, Q, R sont alignés si et seulement si (AA'), (BB'), (CC') sont concourantes.

Preuve On choisit la droite (PQ) comme droite à l'infini et on se ramène à la version affine du théorème.

6.2 Théorème de Pappus et commutativité

Le théorème de Pappus est vrai dans $P_2(K)$ lorsque K est commutatif.

Enoncé(affine) Soient D et D' deux droites affines distinctes dans un plan affine, dont le corps associé est commutatif. Soient A, B, C ∈ D et A', B', C' ∈D' tels que (AB')//(A'B) et (BC')//(B'C). Alors, (CA')//(C'A).

Preuve

- Cas 1 :supposons D non parallèle à D'. Posons O = D∩D'
  Soit h_1 l'homothétie de centre O telle que h_1(A)=B.
  Soit h_2 l'homothétie de centre O telle que h_2(B) = C.
  Alors h_1(B')=A'(car (AB')//(BA0)) et h_2(C')=B' car (BC')//(B'C).
  Comme K est un corps commutatif, $h_1\ h_2 = h_2\ h_1$. Posons h_3 cette homothétie.
  h_3(A) = $h_2\ h_1$(A) = h2(B) = C.
  h_3(C') = $h_1\ h_2$(C')=h_1(B') = A'.
  Finalement (AC') a pour image (A'C). L'homothétie conserve le parallélisme, d'où le résultat.
- Cas 2 :supposons D parallèle à D'. On procède de la même manière en composant les translations de vecteur $\overrightarrow{AB} = \overrightarrow{B'A'}$ et $\overrightarrow{BC} = \overrightarrow{C'B'}$.
  On a alors : $\overrightarrow{AC} = \overrightarrow{AB}\ \overrightarrow{BC} = \overrightarrow{B'A'} + \overrightarrow{C'B'} = \overrightarrow{C'A'}$ donc $\overrightarrow{AC} = \overrightarrow{C'A'}$.
  Finalement,(AC')//(A'C).

Enoncé(projectif) Soient D et D' deux droites projectives distinctes dans le plan projectif. Supposons que A, B, C ∈ $D\backslash D0$ et A', B', C' ∈ $D'\backslash D$, A, B, C distincts 2 à 2, A', B', C' distincts2 à 2. Alors les points (AB') ∩ (A'B), (BC') ∩ (B'C) et (CA') ∩ (C'A) sont alignés.

Preuve On se ramène au cas affine en prenant la droite $(\alpha\beta)$ où $\alpha = (A'B) \cap (AB')$ et $\beta = (BC') \cap (B'C)$ comme droite à l'infini.

Remarque En regardant la preuve, on remarque qu'il y a équivalence entre $P_2(K)$ vérifie Pappus et K commutatif.

7 Les seuls plans arguésiens sont les plans projectifs usuels

7.1 Si on suppose le théorème de Desargues vrai...

Rappel de l'énoncé (axiome de Desargues) Si ABC et A'B'C' sont deux triangles (c'est-à-dire A, B, C et A', B', C' ne sont pas alignés, $A \neq A'$, $B \neq B'$, $C \neq C'$, $(AB) \neq (A'B')$, $(BC) \neq (B'C')$, $(CA) \neq (C'A')$, la droite (AA') ne contient aucun des points B, B', C, C' et de même pour les lettres B et C). Alors (AA'), (BB'), (CC') sont concourantes si et seulement si $(AB) \cap (A'B')$, $(BC) \cap (B'C')$, $(CA) \cap (C'A')$ sont alignés.

Remarque Les deux sens du théorème de Desargues sont duaux l'un de l'autre. On peut d'ailleurs remarquer qu'ils sont équivalents modulo les axiomes d'un plan projectif général.

7.1.1 Existence de perspectives

Soit Π un plan projectif général.

Si on suppose qu'il existe une perspective f d'axe d, de centre O et qui envoie A sur A', pour un point A différent de O et qui ne se trouve pas sur d, on voit immédiatement que f est la seule perspective à vérifier ces propriétés. C'est-à-dire qu'une perspective est uniquement déterminée par son axe, son centre et l'image d'un point extérieur à l'axe et au centre.

On remarque que pour un plan projectif usuel, étant donné une droite d, un point O, un point A différent de O et tel que $A \notin d$ et un point $A' \in (OA)$ différent de O et de A et tel que $A' \notin d$, il existe toujours une perspective d'axe d, de centre O et qui envoie A sur A'. On se dit qu'il est raisonnable de demander à un plan cette propriété d'existence, si on veut avoir un plan plus ou moins raisonnable.

On va voir que cette propriété suffit pour qu'un plan soit plan projectif usuel.

Soit une droite d, un point O.

Axiome des perspectives $O-d$ (propriété de transitivité) Soit un point A différent de O et tel que $A \notin d$ et un point $A' \in (OA)$ différent de O et de A et tel que $A' \notin d$, alors il existe une perspective d'axe d, de centre O et qui envoie A sur A'.

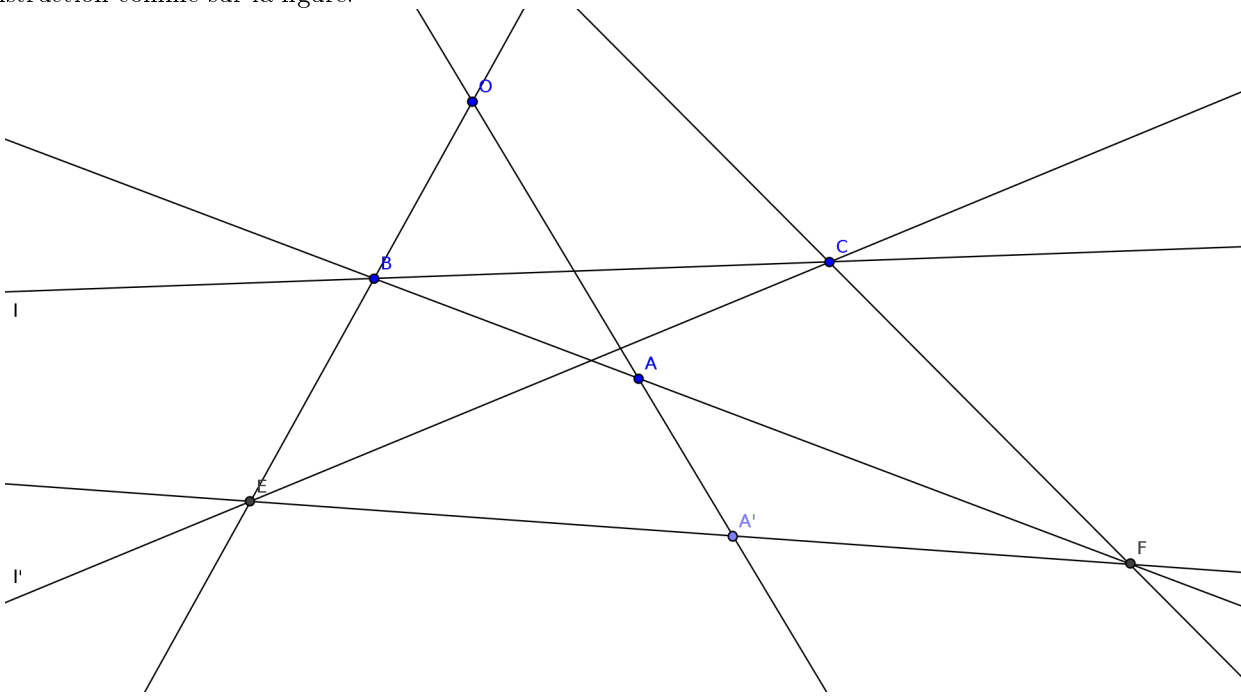
Terminologie On dit qu'une plan est $O-d$ transitif lorsqu'il vérifie l'axiome des perspectives $O-d$. On dira qu'un plan vérifie l'axiome des perspectives lorsqu'il est $O-d$ transitif pour tout point O et toute droite d.

7.1.2 Formes équivalentes de l'axiome des perspectives

Axiome des perspectives* Soit un point O, un point A différent de O, un point $A' \in (OA)$ différent de O et de A, une droite l ne passant pas par A ni par O et une droite l' ne passant pas par A' ni par O et différente de l, alors il existe une perspective de centre O et qui envoie A sur A' et l sur l'.

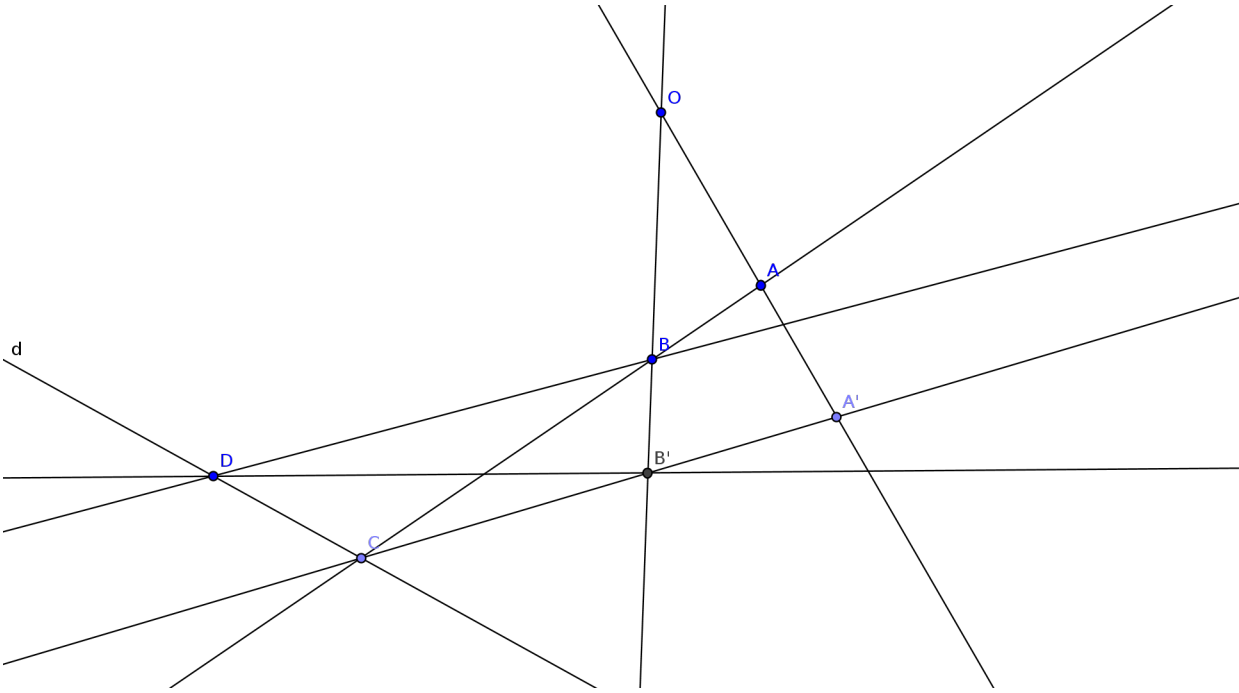
On voit facilement qu'une perspective ainsi définie est unique.

Perspective $\Rightarrow$ Perspective* On se donne O, A, A', l, l'. On réalise la construction comme sur la figure.



On sait qu'il existe une perspective d'axe (FC), de centre O qui envoie A sur A'. Il suffit de montrer qu'elle envoie l sur l'. Par construction, le point B est envoyé sur le point E, et le point C est fixe. D'où le résultat.

Perspective* $\Rightarrow$ Perspective On se donne O, d, A, A'. On réalise la construction comme sur la figure.



On sait qu'il existe une perspective de centre O, qui envoie A sur A' et (DB) sur (DB'). Il suffit de montrer que son axe est d. Or, par construction, elle fixe les points D et C.

7.1.3 Axiome des perspectives ⇒ Axiome de Desargues

Soient ABC et A'B'C' deux triangles tels que (AA'), (BB'), (CC') concourent en O. Il existe alors une perspective de centre O qui envoie A sur A' et (BC) sur $(B'C')$. Cette perspective envoie donc B sur B' et C sur C'. Cette perspective envoie (AB) sur $(A'B')$ et (CA) sur $(C'A')$. Donc, les points $(AB) \cap (A'B')$, $(BC) \cap (B'C')$, $(CA) \cap (C'A')$ se trouvent sur l'axe de la perspective et donc sont en particulier alignés.

7.1.4 Axiome de Desargues ⇒ Axiome des perspectives

Soit la configuration de l'**axiome des perspectives**. Soit B un point extérieur à (OA) et à d. On définit le point $B'' = (AB) \cap d$ et puis le point $B' = (A'B'') \cap (OB)$. On définit une application f du plan dans lui-même, dont le caractère bijectif est immédiat, en disant que O et tous les points de d sont fixes. Pour un point C extérieur à (OA) et à d, on construit $f(C)$ comme on construit B' à partir de B. Enfin, on la définit sur (OA) à partir des points B, B'. En particulier, $f(A) = A'$ et $f(B) = B'$.

Il reste à montrer que f est une collinéation.

Soient X, Y deux points non alignés avec O et extérieurs à d. On montre que le point d'intersection de (XY) et (f(X)f(Y)) se trouve sur d. Il y a plusieurs cas

à distinguer et le théorème de Desargues à utiliser.

Soient P_1, P_2, P_3 trois points alignés. Si (P_1P_2) passe par O ou est égale à la droite d, le fait que les images sont alignées est clair. Si un des points appartient à d c'est le paragraphe précédent. Si ce n'est pas le cas, il suffit de nommer P_4 le point d'intersection de (P_1P_2) et d, et de considérer les parties à trois éléments de $\{P_1, P_2, P_3, P_4\}$ contenant P_4.

Raffinement En regardant la preuve, on remarque l'équivalence pour une droite l et un point O : un plan est $O-l$ transitif SSI pour toute paire de triangles pour lesquels les droites joignant les sommets correspondants se coupent en O et les points d'intersections entre deux des trois paires de côtés correspondants se trouvent sur l alors le point d'intersection de la troisième paire de côtés correspondants se trouve sur l (petit $O - l$ Desargues).

7.1.5 Axiome des perspectives ⇒ Plan projectif usuel

Soit Π un plan projectif général vérifiant l'axiome des perspectives (ou l'axiome de Desargues, c'est pareil). On va montrer que c'est un plan projectif usuel sur un corps.

On va commencer par choisir une droite d du plan.

Structure de groupe abélien sur $\Pi\backslash d$ Notons T le groupe abélien des translations d'axe d. Soit $A \in \Pi\backslash d$. On identifie chaque point de $\Pi\backslash d$ avec la translation qui envoie A sur ce point. On a ainsi une structure de groupe abélien sur $\Pi\backslash d$, dont l'élément neutre est A, et dont on notera la loi $+$.

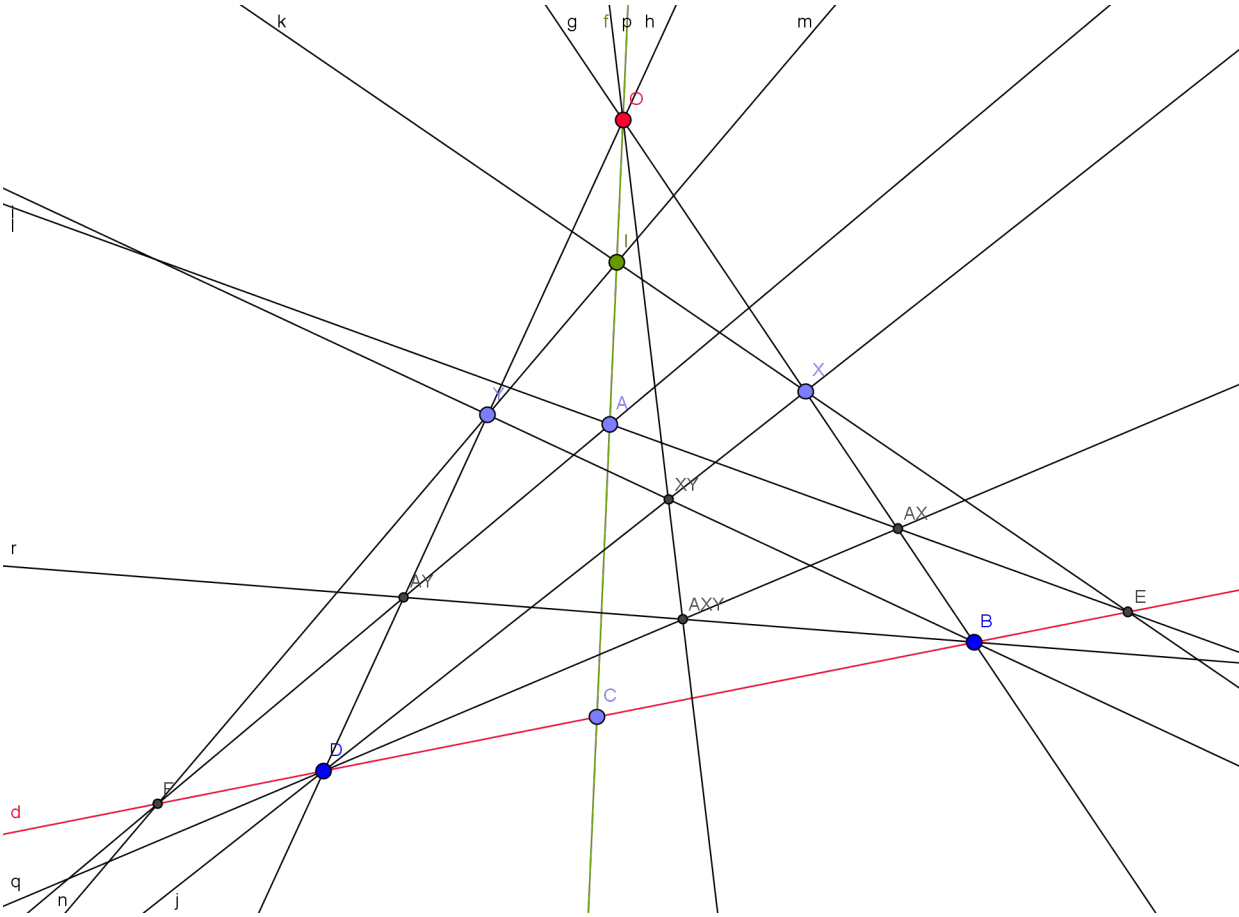
Construction du corps : définition de l'ensemble sous-jacent Soit l une droite qui passe par A. On pose $K = l\backslash(l \cap d)$. On pose $0 = A$. On choisit un point $1 \in K\backslash\{0\}$.

Construction du corps : définition de la structure additive K est un sous-groupe de $\Pi\backslash d$ pour la loi $+$ définie ci-dessus.

Construction du corps : définition de la structure multiplicative Pour $a \in K\backslash\{0\}$, on note h_a la perspective d'axe d, de centre A qui envoie 1 sur a (qui éventuellement est l'identité).

On identifie ainsi chaque point de $a \in K\backslash\{0\}$ avec h_a. Ainsi, on a identifié K^* avec le groupe des perspectives d'axe d et de centre A, qui permet de munir K^* d'une loi de groupe avec 1 pour élément neutre. Ceci nous permet de munir K d'une loi de multiplication.

Construction du corps : vérification des axiomes de corps non trivialement vérifiées On veut $a(b + c) = ab + ac$. Pour cela il suffit de montrer que $\forall a \in K\backslash\{0\}\ \forall x, y \in \Pi\backslash d\ h_a(x + y) = h_a(x) + h_a(y)$. Si (xy) ne passe pas par A, la preuve est résumée par la figure suivante :



Si (xy) passe par A, on dispose de $u \in \Pi\backslash d$ tel que $u \notin (xy)$. On a que $x+y \in (xy)$. Puis, en utilisant le 1er cas, $h_a(x+y+u) = h_a(x) + h_a(y+u) = h_a(x) + h_a(y) + h_a(u)$ et $h_a(x+y+u) = h_a(x+y) + h_a(u)$. Ce qui termine la preuve.

On veut aussi $(b+c)a = ba + ca$. Pour cela il suffit de montrer que $\forall a, b \in K\backslash\{0\}$ $\forall x \in \Pi\backslash d$ $h_{a+b}(x) = h_a(x) + h_b(x)$. On peut supposer que $x \notin K$. On a $(1x)$, $(ah_a(x))$ et $(bh_b(x))$ sont concourantes en un point P de d. Donc, les translations correspondant à $x-1$, $h_a(x)-a$ et $h_b(x)-b$ ont toutes pour centre P. Donc, la translation correspondant à $h_a(x)+h_b(x)-(a+b)$ a pour centre P. Ainsi, $h_a(x) + h_b(x)$ est le point d'intersection de (Ax) et de la droite joignant $a+b$ à P, c'est donc $h_{a+b}(x)$.

Rien d'autre à vérifier.

Construction de l'espace projectif usuel isomorphe à Π On remarque d'abord que le groupe abélien $\Pi\backslash d$ peut être muni d'une loi de composition à gauche par un élément de K. Pour $a \in K$ et $x \in \Pi\backslash d$, on pose $ax = h_a(x)$. $\Pi\backslash d$ est ainsi muni d'une structure d'espace vectoriel à gauche sur K. Les droites

vectorielles de l'espace vectoriel ainsi défini sont les restrictions à $\Pi \backslash d$ des droites passant par A. Les droites affines (translatées des droites vectorielles) sont les restriction à $\Pi \backslash d$ des droites autres que d (translatées des droites passant par A). On voit enfin que l'espace vectoriel obtenu est de dimension 2.

Par rajout de la droite à l'infini, Π est bien le plan projectif usuel sur le corps K.

Remarque Dans la preuve, on s'est uniquement servis de l'existence de toutes les perspectives possibles d'un axe fixé. On peut en déduire une propriété géométrique intéressante, plus précisément l'équivalence entre les deux assertions suivantes :

- Il existe une droite d telle que pour tout point O, pour tout point A différent de O et n'appartenant pas à d et pour tout point $A' \in (OA)$ différent de O et de A et n'appartenant pas à d, il existe une perspective d'axe d, de centre O qui envoie A sur A'
- Pour toute droite d telle que pour tout point O, pour tout point A différent de O et n'appartenant pas à d et pour tout point $A' \in (OA)$ différent de O et de A et n'appartenant pas à d, il existe une perspective d'axe d, de centre O qui envoie A sur A' (axiome des perspectives)

Autrement dit, être $O - d$ transitif pour tous les O et tous les d est équivalent à être $O - d$ transitif pour un certain d et pour tous les O.

Néanmoins, prenons garde au fait qu'être un plan à translations pour une droite n'est pas équivalent à être un plan à translation pour toutes les droites.

7.2 Si on suppose de plus le théorème de Pappus

Un plan projectif usuel vérifie Pappus si et seulement si le corps de base est commutatif. Voyons ce qui se passe lorsqu'un plan projectif général vérifie seulement Pappus.

7.2.1 Théorème de Hessenberg

Un plan qui vérifie le théorème de Pappus vérifie aussi le théorème de Desargues. Par conséquent, un plan projectif général qui vérifie le théorème de Pappus est un plan projectif usuel sur un corps commutatif.

7.3 Lorsque le corps de base est fini...

7.3.1 Théorème de Wedderburn

Énoncé Tout corps fini est commutatif.

Preuve

1. Soit K un corps, on note Z son centre,
   $Z := \{x \in K, \forall y \in K \; xy = yx\}$
   Z est un sous-corps de K qui est commutatif et K est un espace vectoriel

sur Z, alors si on note q=$|Z|$, alors $|K| = q^d$ pour un certain entier d et il suffit de monter d=1.
Soit $x \in K$, on note $Z_x := \{y \in K,\ xy = yx\}$ on a les extensions de corps suivantes :
$Z \subset Z_x \subset K$ et alors $|Z_x| = q^{d_x}$ pour un entier d_x et $d_x | d$.

2. K^* agit sur lui même par conjugaison, les éléments de K^* avec une orbite réduite à un point sont exactement les éléments du centre privé de 0, soient $x_1, ..., x_n$ des représentants des orbites non réduites à un point, la formule des classes donne alors :
$|K^*| = |Z| - 1 + \sum_{k=1}^{n} \frac{|K^*|}{|stab(x_k)|}$
soit :
$q^d - 1 = q - 1 + \sum_{k=1}^{n} \frac{q^d - 1}{q^{d_{x_k}} - 1}$
3. On définit pour $k \in \mathbb{N}$ le k-ième polynôme cyclotomique
$\phi_k := \prod_{r \wedge k = 1} X - exp(\frac{2ir\pi}{k})$
Alors, ϕ_k est à coefficients entiers, et on a $\forall k \in \{1, ..., n\}$, $\phi_d | \frac{X^d - 1}{X^{d_{x_k}} - 1}$ dans $\mathbb{Z}[X]$ d'où $\phi_d | F(X)$
où $F(X) := X - 1 + \sum_{k=1}^{n} \frac{X^d - 1}{X^{d_{x_k}} - 1}$
cela implique l'existence d'un entier m tel que $m\phi_d(q) = F(q) = q - 1$ d'où $|\phi_d(q)| \leq q - 1$ or $|\phi_q| = \prod_{r \wedge k = 1} |q - exp(\frac{2ir\pi}{k})|$
Or $|q - exp(\frac{2ir\pi}{k})| > q - 1$ *si* $r \neq 1$
d'où d=1 et K commutatif.

7.3.2 Conséquences pour les plans projectifs finis

On en déduit qu'un plan projectif général fini qui vérifie le théorème de Desargues vérifie aussi le théorème de Pappus.

Deuxième partie

Affaiblissement du système d'axiomes et apparition des algèbres d'octonions

Définition Un plan projectif général est dit à translations lorsque pour toute droite d, le groupe des translations d'axe d agit transitivement sur l'ensemble des points extérieurs à d.

Remarque Si A, B sont deux points distincts de d, et si on suppose que le plan est à la fois $A-d$ transitif et $B-d$ transitif, alors le groupe des translations d'axe d agit transitivement sur l'ensemble des points extérieurs à d.

L'énoncé dual est : si a, b sont deux droites discinctes se coupant en D, et si on suppose le plan à la fois $D-a$ transitif et $D-b$ transitif, alors le groupe des translations de centre D agit transitivement sur les droites ne passant pas par D.

Définition Un plan projectif est dit à translations par rapport à une droite d lorsque le groupe des translations d'axe d agit transitivement sur l'ensemble des points extérieurs à d.

8 Un plan à translations est un plan sur un anneau alterné à division

Soit Π un plan à translations. On peut alors choisir une droite d, et définir une structure de groupe abélien G sur $\Pi\backslash d$ d'origine O, comme dans la partie 1. On choisit une droite l passant par O, et on s'intéresse au sous-groupe de G constitué des éléments de $l\backslash d$. Chaque point de la droite $l\backslash d$ est muni de coordonnées correspondantes $(g:g:1)$, avec O ayant pour coordonnées $(0:0:1)$, et un autre point I ayant pour coordonnées $(1:1:1)$. Le point à l'infini de l est muni de coordonnées $(1:1:0)$. On choisit encore deux points sur la droite à l'infini : l'origine X de coordonnées $(1:0:0)$ et le point à l'infini Y de coordonnées $(0:1:0)$. Ensuite, le point d'intersection entre la droite joignant $(1:0:0)$ et $(b:b:1)$ et la droite joignant $(0:1:0)$ et (a :a :1) a pour coordonnées $(a:b:1)$. Enfin, le point à l'infini de la droite joignant (0 :0 :1) et (1 :m :1) a pour coordonnés (1 :m :0). On vérifie que par ce procédé, on munit de façon non ambigue, le plan Π d'un système de coordonnées. On définit sur G une loi multiplicative par pour $x, m \in G$, xm vérifie $(x:xm:1)$ appartient à la droite joignant $(0:0:1)$ et $(1:m:0)$. On vérifie que les droites autres que la droite à l'infini ont soit pour équation $x=c$ soit pour équation $y=xm+b$. On vérifie que $(x:y:1)+(x':y':1)=(x+x':y+y':1)$ pour la loi de groupe définie sur $\Pi\backslash d$. On vérifie ensuite la validité de toutes les identités qu'on veut une à une pour montrer que G muni des deux loi est un anneau alterné à division.

9 Plan projectifs sur un anneau alterné à division

Définition Soit A un ensemble contenant au moins deux éléments et muni d'une loi de composition interne notée additivement et d'une loi de composition interne notée multiplicativement. On dit que A est une algèbre alternée à division lorsque :

— $(A,+)$ est un groupe abélien de neutre 0.

— La multiplication est distributive à droite et à gauche par rapport à l'addition.

— Une forme d'associativité faible est vérifiée : $(xx)y = x(xy)$ et $y(xx) = (yx)x$
— La multiplication possède un neutre bilatère noté 1
— Tout élément $a \neq 0$ possède un inverse bilatère pour la multiplication.

Propriété On peut montrer que l'inverse de tout élément est unique, qu'il n'y a pas de diviseurs de zéro, que pour tous $a, b \neq 0$ $a^{-1}(ab) = b = (ba)a^{-1}$ et $(ab)^{-1} = b^{-1}a^{-1}$. C'est fait dans ce document dans la partie consacrée à la démonstration du théorème d'Artin-Zorn.

Construction A^3 est naturellement munie d'une loi additive qui en fait un groupe abélien et d'une multiplication à gauche par un scalaire de A. La multiplication par un scalaire est distributive à gauche par rapport à l'addition de A^3 et à droite par rapport à l'addition de A. Enfin, 1 est neutre à gauche pour la multiplication par un scalaire. Tous les axiomes d'espace vectoriel sont donc vérifiées sauf celles liées à l'associativité. On dira quand même que A^3 est muni d'une structure d'**espace vectoriel sur algèbre à division**.

On ne peut pas définir $P_2(A)$ par le même procédé que pour les corps, car la relation « être collinéaire » sur les vecteurs non nuls n'est pas une relation d'équivalence, car l'associativité manque. On va procéder autrement.

Définition Soit $(x, y, z) \in A^3 \backslash \{(0, 0, 0)\}$. Alors, on note $(x : y : z)$ l'ensemble des vecteurs non nuls collinéaires à (x, y, z). Il s'agit donc de (x, y, z) à constante multiplicative à gauche non nulle près.

Définition On pose $P_2(A) = \{(x : y : 1)/x, y \in A\} \cup \{(1 : x : 0)/x \in A\} \cup \{(0 : 1 : 0)\}$. Il s'agit d'une union disjointe qui réalise une partition de $A^3 \backslash \{0\}$. C'est une union disjointe de trois ensemble qu'on peut voir ainsi : les points à distance finie, les points à distance finie de la droite à l'infini, le point à l'infini de la droite à l'infini.

Définition Les droites de $P_2(A)$ sont les parties suivantes de $P_2(A)$:
— la droite à l'infini : $\{(1 : x : 0)/x \in A\} \cup \{(0 : 1 : 0)\}$
— pour chaque $a \in A$, la droite passant par $(a : 0 : 1)$ et le point à l'infini de la droite à l'infini : $\{(a : y : 1)/y \in A\} \cup \{(0 : 1 : 0)\}$
— pour chaques $b, m \in A$, la droite de pente m et d'ordonnée à l'origine b : $\{(x : xm + b : 1)/x \in A\} \cup \{(1 : m : 0)\}$

On a donc choisi de définir les droites par leur équation.

10 Un plan projectif sur un anneau alterné à division est un plan à translations

On vérifie aisément que $P_2(A)$ vérifie les axiomes (P1) et (P2). Il vérifie (P3) : il suffit de choisir les points :

— $(1:0:0)$: origine de la droite à l'infini
— $(0:1:0)$: point à l'infini de la droite à l'infini
— $(0:0:1)$: origine de l'ensemble des points à distance fini
— $(1:1:1)$: la droite qui joint ce point à (0 :0 :1) coupe la droite à l'infini en (1 :1 :0)

On a donc que c'est un plan. Il reste à montrer qu'on a un plan à translations.

On note l la droite à l'infini.

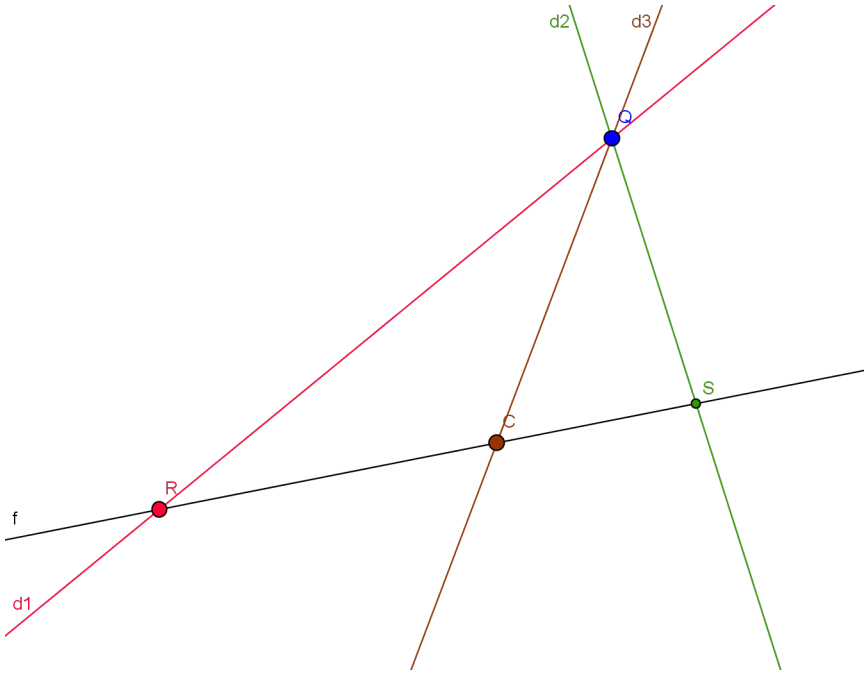
10.1 Les translations d'axe la droite à l'infini agissent transitivement sur les points à distance finie.

Soient $A = (x : y : 1)$ et $A' = (x' : y' : 1)$ deux points à distance finie. On va construire une translation d'axe la droite à l'infini qui envoie A sur A'. On définit le vecteur de la translation par $(a, b) = (x' - x, y' - y)$. Alors, pour tout point à distance finie (u :v :1), on définira l'image par (u+a :v+b :1). Tout point de la droite à l'infini est fixe. Il reste à montrer que la bijection du plan définie ainsi est bien une collinéation. Mais, la droite à l'infini est fixée. Une droite d'équation $x = p$ est envoyée sur la droite d'équation $x = p + a$. Une droite d'équation $y = xm + c$ est envoyé sur la droite d'équation $y = xm - bm + a + c$. Ceci termine la preuve.

10.2 C'est un plan à translations par rapport à toute droite qui passe par le point à l'infini de la droite à l'infini

Propriété Soit un plan projectif qui est un plan à translations par rapport à une droite d_1 et par rapport à une autre droite d_2. Soit Y le point d'intersection de d_1 et d_2. Alors c'est un plan à translations par rapport à toute droite passant par Y.

Preuve Soit un plan projectif vérifiant les hypothèses de l'énoncé.



On veut montrer qu'on a un plan à translations par rapport à la droite d_3. On a une translation d'axe d_1 et de centre R qui evoie S sur C. Elle échange les translations de centre S et d'axe d_2 et les transations de centre C et d'axe d_3. Or, on a la $S - d_2$ transitivité. Donc, $C - d_3$ transitivité. Il suffit de faire la même chose pour un autre point C' de d_3 pour conclure.

Conséquence Il suffit donc de montrer qu'on a un plan à translations par rapport à une droite qui passe par le point à l'infini de la droite à l'infini mais qui n'est pas la droite à l'infini. Or, le plan est déjà transitif par rapport à la droite à l'infini. Donc, il suffit de montrer qu'il existe une collinéation qui envoie la droite à l'infini sur une autre droite qui passe par le point à l'infini de la droite à l'infini.

Définition de la collinéation On la définit de la façon suivante :

- $(0:1:0) \longmapsto (0:1:0)$
- $(1:m:0) \longmapsto (1:m:1)$
- $(-1:m:1) \longmapsto (1:-m:0)$
- $(0:b:1) \longmapsto (0:b:1)$
- $(c:d:1) \longmapsto ((1+c^{-1})^{-1}:(1+c^{-1})d:1)$ si $c \neq 0, -1$

On vérifie que c'est une collinéation.

10.3 On a un plan à translation

Il suffit de trouver une collinéation qui ne fixe pas (0 :1 :0) :

— $(a : b : 1) \longmapsto (b : a : 1)$
— $(1 : 0 : 0) \longmapsto (0 : 1 : 0)$
— $(1 : m : 0) \longmapsto (1 : m^{-1} : 0)$ pour $m \neq 0$
On vérifie que c'est une collinéation.

10.4 Remarque

On peut montrer que A est associatif SSI le théorème de Desargues est vrai.

Troisième partie
Classification des plans projectifs à translation, étude des plans finis

On veut pouvoir classer les plans qu'on a défini à isomorphisme par collinéation près. Bien entendu, les axiomes géométriques sont préservées par collinéation.

11 Cas des plans arguésiens

On peut se servir de la structure linéaire de $P_2(K)$ uniquement pour donner une autre définition (dans un certain sens plus simple) de la notion d'automorphisme de $P_2(K)$, et voir à quel point cell-ci est équivalente à celle donnée plus haut. On va voir que $P_2(K)$ et $P_2(K')$ peuvent être isomorphes au sens défini plus haut (au sens des collinéations) si K et K' ne sont pas isomorphes.

11.1 Définition

Soit $f \in GL_3(K)$, alors f passe au quotient définissant $P_2(K)$. On observe qu'on obtient ainsi un automorphisme de $P_2(K)$ au sens défini ci-dessus. Le groupe des automorphimes de $P_2(K)$ ainsi défini se note $PGL_3(K)$. On remarque que chaque élément se représente par un élément de $GL_3(K)$ à une constante par multiplication à droite près.

Repère projectif Un repère projectif est un quadrangle. Dans un base adaptée de K^3, on peut toujours l'écrire (1 :0 :0), (0 :1 :0), (0 :0 :1), (1 :1 :1). Un élément de $PGL_3(K)$ envoie un repère projectif sur un repère projectif. Son intérêt est que $PGL_3(K)$ agit de manière simplement transitive sur les repères projectifs de $P_2(K)$.

11.2 Non équivalence des définitions

On peut facilement trouver d'autres automorphismes dans certains cas. Soit K et K' deux corps. On dira qu'une application $f : K^3 \to K'^3$ est semi-linéaire lorsqu'il existe un isomorphisme de corps $\lambda : K \to K'$ tel que :

1) $\forall x, y \in K^3 \ f(x+y) = f(x) + f(y)$

2) $\forall \alpha \in K \ \forall x \in K^3 \ f(\alpha x) = \lambda(\alpha) f(x)$

Un isomorphisme semi-linéaire induit une collinéation.

Avec $K = \mathbb{C}$, on peut trouver des automorphismes semi-linéaires non linéaires qui fixent le repère projectif canonique mais n'induisent pas l'identité.

11.3 Théorème fondamental de la géométrie projective

Toute collinéation σ de $P_2(K)$ est induit par un automorphisme semi-linéaire f de K^3.

Énoncé Soit $\sigma : P_2(K) \to P_2(K')$ une collinéation. Il existe un isomorphisme semi-linéaire $f : K^3 \to K'^3$ qui induit σ. En particulier, les corps K et K' sont isomorphes.

Preuve e_1, e_2, e_3 base de K^3.

1) On montre par récurrence sur r que si $P \subseteq P_1 + ... + P_r$ où $P, P_1, ..., P_r \in P_2(K)$, alors $\sigma(P) \subseteq \sigma(P_1) + ... + \sigma(P_r)$. L'initialisation pour $r = 2$ vient du fait queσ est une collinéation.

2) Soit $P \in P_2(K)$, alors $P \subseteq Ke_1 + Ke_2 + Ke_3$. Puis $\sigma(P) \subseteq \sigma(Ke_1) + \sigma(Ke_2) + \sigma(Ke_3)$. Or, tout point de $P_2(K')$ s'écrit comme un $\sigma(P)$. On pose $g_1, g_2, g_3 \in K'^3$ tels que $\sigma(Ke_i) = K'g_i$ pour $i = 1, 2, 3$ et $\sigma(K(e_1 + e_i)) = K'(g_1 + g_i)$ pour $i = 2, 3$. On a en particulier que g_1, g_2, g_3 est une base de K'^3.

3) On définit $\lambda : K \to K'$ par pour $x \in K$, $\lambda(x)$ est l'unique élément de K' tel que $\sigma(K(e_1 + xe_2)) \subseteq K'(g_1 + \lambda(x)g_2)$. L'injectivité de σ implique l'injectivité de λ. De plus. $\lambda(1) = 1$ et $\lambda(0) = 0$.

De même, on définit $\mu : K \to K'$ par pour $x \in K$, $\mu(x)$ est l'unique élément de K' tel que $\sigma(K(e_1 + xe_3)) \subseteq K'(g_1 + \mu(x)g_3)$.

Soit $x \neq 0$ un élément de K. $K(xe_2 - xe_3) = (Ke_2 + Ke_3) \cap (K(e_1 + xe_2) + K(e_1 + xe_3))$. D'où, $\sigma(K(xe_2 - xe_3)) = (K'g_2 + K'g_3) \cap (K'(g_1 + \lambda(x)g_2) + K'(g_1 + \mu(x)g_3)) = K'(\lambda(x)g_2 - \mu(x)g_3)$. Or, $\sigma(K(xe_2 - xe_3)) = \sigma(K(e_2 - e_3)) = K'(\lambda(1)g_2 - \mu(1)g_3) = K'(g_2 - g_3)$.

Donc, $\forall x \in K \ \lambda(x) = \mu(x)$.

4) Soit $x_2, x_3 \in K$. Alors, $\sigma(K(e_1 + x_2e_2 + x_3e_3)) \subseteq \sigma(K(e_1 + x_2e_2) + \sigma(Ke_3) = K'(g_1 + \lambda(x_2)g_2) + K'g_3$. Et, $\sigma(K(e_1 + x_2e_2 + x_3e_3)) \subseteq \sigma(K(e_1 + x_3e_3) + \sigma(Ke_2) = K'(g_1 + \lambda(x_3)g_3) + K'g_2$. D'où, $\sigma(K(e_1 + x_2e_2 + x_3e_3)) \subseteq K'(g_1 + \lambda(x_2)g_2 + \lambda(x_3)g_3)$.

5) On montre que $\sigma(K(x_2e_2 + x_3e_3)) = K'(\lambda(x_2)g_2 + \lambda(x_3)g_3)$.

6) Soit $y \in K'$. L'antécédent parσ de $K'(g_1 + yg_2)$ est de la forme $K(e_1 + x_2e_2 + x_3e_3)$. Alors, $\lambda(x_2) = y$ et $\lambda(x_3) = 0$, donc $x_3 = 0$. Ainsi, λ est surjective.

7) On démontre que $\lambda(x+y) = \lambda(x) + \lambda(y)$ en considérant l'image par σ de $K(e_1 + (x+y)e_2 + e_3)$.

8) On démontre que $\lambda(xy) = \lambda(x)\lambda(y)$ en considérant l'image par σ de $K(e_1 + (xy)e_2 + xe_3)$.

9) $\lambda : K \to K'$ est donc un isomorphisme de corps. On en déduit que $\sigma(K(x_1e_1 + x_2e_2 + x_3e_3)) = K'(\lambda(x_1)g_1 + \lambda(x_2)g_2 + \lambda(x_3)g_3)$.

10) On définit $f : K^3 \to K'^3$ par $f(e_i) = g_i$ pour $i = 1, 2, 3$ et f semi-linéaire par rapport à l'isomorphisme λ.

12 Cas des plans à translation

La preuve du théorème fondamental de la géométrie projective ne s'étend pas à $P_2(A)$ où A est une algèbre alternée à division. L'unicité de A pour un plan projectif donné est une conséquence non triviale du théorème de Bruck-Kleinfeld.

13 Théorème de Artin-Zorn

Rappel Un anneau alterné R est un ensemble qui vérifie toutes les propriétés d'un anneau sauf éventuellement l'associativité de la deuxième loi, celle-ci est remplacé par une associativité faible :

$$\forall x, y \in R, x(yy) = (xy)y$$
$$\forall x, y \in R, x(xy) = (xx)y$$

Un tel ensemble est dit à division s'il existe un élément neutre et que tout élément admets un inverse :

$$\forall x \in R \setminus \{0\}, \exists y \, xy = yx = 1$$

On aura alors :

$$\forall x, y \in R, (xy = 1 => \forall z \in R, x(yz) = (xy)z = z)$$

Attention, ceci est vrai, mais non élémentaire.

Enoncé Tout anneau alterné à division fini est un corps.

Remarques et plan de la démonstration Ce théorème montre que les plans à translations finis vérifient Desargues et Pappus. La démonstration est axée autour des idées suivantes :

- Un anneau alterné à divisions finis est engendré par un nombre fini d'éléments, et s'il est engendré par un seul élément, c'est un corps.
- Tout sous-anneau engendré par deux éléments est associatif.
- Un corps fini est engendré par un seul élément.

— Si R est engendré par plusieurs éléments, on va montrer qu'on peut baisser le nombre de générateurs. Le sous-anneau engendré par les deux premiers générateurs est associatif, et on montrera que c'est un corps. Il sera alors engendré par un seul élément, et on pourra conclure.

Lemme 1 On pose $(x,y,z) = (xy)z - x(yz)$

1. $(x,x,y) = 0 = (x,y,y)$
2. $(x,y,z) = -(y,x,z) = (y,z,x) = -(z,y,x)$
3. $(x,y,z) = 0$ dès que 2 éléments sont égaux, en particulier xyx=x(yx)=(xy)x
4. $x(y,z,u) - (xy,z,u) + (x,yz,u) - (x,y,zu) + (x,y,z)u = 0$
5. (ab,b,c)=b(a,b,c),(a,b,ca)=a(b,c,a),(ab,c,a)=(a,b,c)a
6. x(yz)x=(xy)(zx)
7. x(y(xz))=(xyx)z

Preuve

1. Immédiat
2. On a $(x+y,x+y,z) = (y,z,x) + (y,x,z) = 0$ Pareil pour les autres.
3. On combine les 2 résultats précédents.
4. On a $x(y,z,u) - (xy,z,u) + (x,yz,u) - (x,y,zu) + (x,y,z)u =$ $x((yz)u) - x(y(zu)) - ((xy)z)u + (xy)(zu) + (x(yz))u - x((yz)u) - (xy)(zu) +$ $x(y(zu)) + ((xy)z)u - (x(yz))u = 0$
5. On applique 4) avec x=a,y=z=b et u=c :$(ab,b,c) = (a,bb,c) - (a,b,bc)$ On applique 4) avec x=y=b,z=c et u=a :$b(b,c,a) = (bb,c,a) - (b,bc,a)$ Or d'après 2), on a :$(b,c,a) = (a,b,c), (bb,c,a) = (a,bb,c) et (b,bc,a) = (a,b,bc)$ Les deux autres formules sont similaires.
6. On a (x,y,zx)=(x,y,z)x, c-à-d (xy)(zx)-x(y(zx))=x(yz)x-x(y(zx)), d'où le résultat
7. On part de la première formule de 5. On permute ab et b, cela donne : (b,ab,c)=-b(a,b,c) (bab)c-b((ab)c)=-b((ab)c)+b(a(bc)) (bab)c=b(a(bc))

Définition Si $x_1, ..., x_n$ sont des éléments de R, on définit par récurrence un monôme en $x_1, ..., x_n$ par :

— Le seul monôme en x_1 est x_1.
— Les monômes en $x_1, ..., x_n$ sont les produits de monômes en $x_1, ..., x_l$ et de monômes en $x_{l+1}, ..., x_n$ pour un l<n.
— Si S est un sous-ensemble de R, on définit $< S >$ le sous-anneau alterné engendré par R, comme l'ensemble des sommes finies de monômes en $x_1, ..., x_n$, où $x_1, ..., x_n$ sont des éléments de S.

Lemme 2 Si R est un anneau alterné, tout sous-anneau alterné engendré par 2 éléments est associatif.

Preuve Par ce qui précède, il suffit de montrer qu'un monôme $M(x_1, ..., x_n)$ est entièrement déterminé par $x_1, ..., x_n$. On va le montrer par récurrence sur n. C'est vrai pour n=1. Soit $n \in \mathbb{N}^*$, et supposons le résultat vrai pour tout k<n. Par définition, il existe un entier l<n tel que $M(x_1, ..., x_n) = M(x_1, ..., x_l)M(x_{l+1}, ..., x_n)$. On va montrer que si l<n-1, on peut trouver un l'>l, avec lequel on aura une décomposition similaire. Alors, par application répétée on aura $M(x_1, ..., x_n) = M(x_1, ..., x_{n-1})x_n$ et le monôme $M(x_1, ..., x_n)$ sera bien uniquement déterminé par $(x_1, ..., x_n)$. On a les trois cas suivants possibles :

1. $x_l = x_{l+1}$
2. $x_l \neq x_{l+1}$ et $x_{l+1} = x_m$
3. $x_l \neq x_{l+1}$ et $x_{l+1} \neq x_m$

Comme S={a,b}, on peut sans perte de généralité se ramener à 3 cas :

1. $x_l = x_{l+1} = a$
2. $x_l = bet x_{l+1} = x_m = a$
3. $x_l = x_m = b$ et $x_{l+1} = a$

1. Posons $x = M(x_1, ..., x_{l-1})$ et $y = M(x_{l+2}, ..., x_n)$ monômes uniquement déterminés par hypothèse de récurrence. On a
   $M(x_1, ..., x_l) = xa$ et $M(x_{l+1}, ..., x_n) = ay$
   Ensuite, (xa)y et x(ay) sont 2 monômes en $x_1, ..., x_{l-1}, x_{l+1}, ..., x_n$ donc sont égaux par hypothèse de récurrence, alors (x,a,y)=0,
   et par le lemme 1, (xa,a,y)=a(x,a,y)=0.
   Alors ((xa)a)y=(xa)(ay), c-à-d $M(x_1, ..., x_l)M(x_{l+1}, ..., x_n) = M(x_1, ..., x_{l+1})M(x_{l+2}, ..., x_n)$
2. Posons $x = M(x_1, ..., x_l)$ et $y = M(x_{l+2}, ..., x_{n-1})$ monômes uniquement déterminés par hypothèse de récurrence. On a
   $M(x_{l+1}, ..., x_n) = axa$
   Ensuite, (xa)y et x(ay) sont 2 monômes en $(x_{l+2}, ..., x_n, x_1, ..., x_l)$ donc sont égaux par hypothèse de récurrence, et alors (x,a,y)=0,
   et par le lemme 1,(y,a,xa)=-(xa,a,y)=a(x,a,y)=0.
   Alors (ya)(xa)=(y(axa)), c-à-d $M(x_1, ..., x_l)M(x_{l+1}, ..., x_n) = M(x_1, ..., x_{l+1})M(x_{l+2}, ..., x_n)$
3. Posons $x = M(x_1, ..., x_{l-1})$ et $y = M(x_{l+1}, ..., x_{n-1})$ monômes uniquement déterminés par hypothèse de récurrence. On a
   $M(x_1, ..., x_l) = xb$ et $M(x_{l+1}, ..., x_m) = yb$
   Ensuite, (xb)y et x(by) sont deux monômes en $x_1, ..., x_{n-1}$, et alors (x,b,y)=0,
   et par le lemme 1, (xb,y,b)=-(xb,b,y)=-b(x,b,y)=0.
   Alors ((xb)y)b=(xb)(yb), c-à-d $M(x_1, ..., x_l)M(x_{l+1}, ..., x_n) = M(x_1, ..., x_{n-1})x_n$

Lemme 3 Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

Preuve Soit n l'ordre du groupe G.

1. Soit d un diviseur de n, et $x \in G$ d'ordre d. On note H le sous-groupe engendré par x. Alors tout élément d'ordre d est dans H, en effet, tout élément de H est racine de $X^d - 1$, et ce polynôme a au plus d racines, donc $\forall y \in G, y^d = 1 => y \in H$.
2. Soit d un diviseur de n, on pose N(d) le nombre d'éléments d'ordre d dans G, si $N(d) \neq 0$, alors soit x d'ordre d, H le sous groupe engendré par x, $H \simeq \mathbb{Z}/d\mathbb{Z}$, et le nombre d'élément d'ordre d dans H est le nombre d'élément d'ordre d dans $\mathbb{Z}/d\mathbb{Z}$, c-à-d le nombre de générateurs de $\mathbb{Z}/d\mathbb{Z}^*$, ce qui vaut $\phi(d)$ où ϕ est l'indicatrice d'Euler.
3. Tout élément de G est d'ordre d pour un d diviseur de n, donc $|G| = n = \Sigma_{d|n} N(d)$. Or $n = \Sigma_{d|n}\phi(d)$, donc $\Sigma_{d|n}(\phi(d) - N(d)) = 0$ et donc $\forall d|n, N(d) = \phi(d)$, en particulier, G admet un élément d'ordre n et est donc cyclique.

Lemme 4 Soit R un anneau alterné, $x \in R$, on désigne par L_x, R_x les applications de multiplication à gauche et à droite par x, et on pose $U_x = L_x R_x = R_x L_x$ bien défini par Lemme 1.

1. x(y,z,xy)+(xy,y,zx)=x(y,z,xy)+(xy)(y,z,x)
2. $L_x L_y L_x = L_{xyx}$
3. $U_{xy} = L_x U_y R_x$, $U_{xy} = R_y U_x L_y$
4. Si $xy = 1$, alors $L_x L_y = R_y R_x = I$, c-à-d $\forall z \in R x(yz) = z = (zx)y$

Preuve

1. On a par le lemme 1 : (x,y,zx)=x(y,z,x), on remplace x par x+w :
   (x+w,y,z(x+w))=(x+w)(y,z,x+w)
   (x,y,zw)+(w,y,zx)=x(y,z,w)+w(y,z,x), on évalue pour w=xy :
   (x,y,z(xy))+(xy,y,zx)=x(y,z,xy)+(xy)(y,z,x)
2. C'est le point 7 du lemme 1.
3. On montre la première identité, la deuxième s'en déduit par symétrie.
   Soit $z \in R$, $(U_{xy} - L_x U_y R_x)z =$
   (xy)(z(xy))-x(y((zx)y)))=(x,y,z(xy))+x(y(z(xy)))-x(y((zx)y)))
   =(x,y,z(xy))-x(y(z,x,y))
   =(x,y,z(xy))-x(y,z,xy) par le point 5 du Lemme 1
   =(xy)(y,z,x)-(xy,y,zx) par le point 1
   =(xy)((yz)x-y(zx))-((xy)y)(zx)+(xy)(y(zx)) =(xy)((yz)x)-((xy)y)(zx) =$(xy)((yz)x) -$
   $(xy^2)(zx) = x(y^2z)x - x(y^2z)x$ par le point 6 du lemme 1
   =0
4. On a $I = U_{xy} = L_x U_y R_x$, d'où $L_x L_y = L_x L_y L_x U_y R_x$
   $= L_{xyx} U_y R_x$ par le point 1
   $= L_x U_y R_x$ car xyx=x
   =I par le point précédent
   L'autre sens se déduit par symétrie.

Preuve du théorème Soit R un anneau alterné à division fini, comme R est fini, il existe $a_1, ..., a_n$ tels que R=$<a_1, ..., a_n>$, montrons le résultat par récurrence sur n. Le cas n=1 est évident.

- Regardons $R_1 =< a_1, a_2 >$. Par le lemme 2, R1 est associatif, on va montrer que c'est un corps. Soit $a \in R_1$, comme R_1 est fini, il existe 2 indices k<k' tels que $a^k = a^{k'}$, et alors $a^k(1 - a^{k'-k}) = 0$ et alors $a^{k'-k} = 1$ par lemme 4, et $1 \in R_1$, et $a^{-1} = a^{k'-k-1} \in R_1$. R_1 est donc un corps et est engendré par un élément b par lemme 3.
- On a alors R=$<b, a_3, ..., a_n>$, et on conclut la récurrence.

13.1 Théorème de Bruck Kleinfeld

Le but de cette section est de montrer le théorème de Bruck Kleinfeld, celui-ci énonce qu'un anneau alterné unitaire à division (de caractéristique différente de 2) qui n'est pas associatif est une algèbre d'octonions, c-à-d un espace vectoriel de dimension 8 sur un corps sous-jacent.
On note (x,y,z) l'associateur comme dans la partie précédente, et (x,y)=xy-yx le commutateur de x et y. On note aussi C(R) le centre de R : C(R)=$\{x \in R, (x, R, R) = 0$ et $(x, R) = 0\}$, et N(R)=$\{x \in R, (x, R, R) = 0\}$

13.1.1 Construction de Cayley-Dickson

Une involution sur un anneau R est un isomorphisme j tel que $j^2 = Id$, on note alors $\overline{a} = j(a)$, cela revient à :

$$\overline{(a+b)} = \overline{a} + \overline{b}$$
$$\overline{ab} = \overline{b}\overline{a}$$
$$\overline{\overline{a}} = a$$

On dit que j est central si $n(a) = a\overline{a}$ et $t(a) = a + \overline{a}$ sont dans le centre de R.
On définit n(a,b)=n(a+b)-n(a)-n(b)=$a\overline{b} + b\overline{a}$
Si R est unitaire, et possède une involution centrale j :$a- > \overline{a}$ et un élément$\zeta = \overline{\zeta}$, alors, on crée l'anneau $CD(R, \zeta)$=R*R avec les lois :
$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)(a_1, a_2)(b_1, b_2) = (a_1b_1 + \zeta b_2\overline{a_2}, \overline{a_1}b_2 + b_1a_2)$

Lemme 1 Soit R un anneau unitaire avec une involution centrale j :$a- > \overline{a}$. Si R est un sous-anneau unitaire d'un anneau alterné S et si $s \in S$ est un élément inversible avec :

- $s^2 =: \zeta \in N(R)$
- $as = s\overline{a}$ pour $a \in R$
- $R \cap sR = 0$

Alors $R \bigoplus sR$ est isomorphe à $CD(R, \zeta)$

Preuve Comme $as^2 = s\overline{a}s = s^2\overline{\overline{a}} = s^2a$ d'où $\zeta \in C(R)$
De plus, comme s est inversible (a,b)->a+sb est une bijection de R*R dans $R \bigoplus sR$.
Ensuite, comme l'anneau est alterné, on a $a(sb) = s(\overline{a}b)$ et $((sa)b)s = (s(ba))s$ d'où (sa)b=s(ba).
Finalement $(sa)(sb) = (sa)(\overline{b}s) = (s(a\overline{b}))s = ((b\overline{a})s)s = (b\overline{a})s^2 = \zeta b\overline{a}$.

13.1.2 Algèbres de composition

Definition Si K est un anneau unitaire, associatif et commutatif, on dit que A est une algèbre sur K si A est un anneau(pas nécessairement associatif) et un K-module à gauche unitaire tel que $\forall \alpha, a, b \in K * A^2, \alpha(ab) = (\alpha a)b = a(\alpha b)$
On dit que A est une algèbre de composition sur un corps K s'il existe une forme quadratique non dégénérée n avec la propriété n(ab)=n(a)n(b).
Si K[u] est une extension quadratique du corps K avec $u^2 = \alpha u - \beta$ avec une involution j donnée par j(u)=$\overline{u} = \alpha - u$. On remarque que la norme n(v)=vj(v) est une forme quadratique avec une matrice de déterminant $\delta = \alpha^2 - 4\beta$. On dit que K[u] est une extension quadratique non dégénérée si $\delta \neq 0$.
Dans ce cas, si $0 \neq \zeta \in K$, on dit que $Q = CD(K[u], \zeta$ est une algèbre de quaternions.
Si Q est une algèbre de quaternions, et que $0 \neq \lambda \in K$, on dit que $\mathbb{O} = CD(Q, \lambda)$ est une algèbre d'octonions.

Lemme 2 Si $A \neq K1$ est une algèbre unitaire sur un corps K, alors, on a la suite d'implication 1.=>2.=>3.

1. A est alternée avec une K-involution j telle que la forme quadratique n(a)=aj(a) est non dégénérée
2. A est une algèbre de composition.
3. A est soit une extension quadratique non dégénérée, soit une algèbre de quaternions ou d'octonions.

Preuve

1. => 2. On a $a + \overline{a} \in K \subset N(A)$. Par le lemme 2 de la partie précédente, toute sous algèbre engendrée par une sous partie de N(A) et 2 éléments de A est associative, ce fait est le Lemme d'Artin. En particulier, la sous-algèbre engendrée par $a, b, \overline{a}, \overline{b}$ est associative. Alors $n(ab) = (ab)(\overline{b}\overline{a}) = an(b)\overline{a} = n(a)n(b)$ d'où l'algèbre est une algèbre de composition.
2. =>3. Maintenant on suppose que $B \neq A$ est une sous-algèbre unitaire de A, que j envoie B sur lui-même et que n n'est pas dégénérée sur B, on a que $A = B \bigoplus B^{\perp}$ et n n'est pas dégénérée sur $B^{\perp}$, alors $\zeta := -n(s) \neq 0$ pour un $s \in B^{\perp}$. Si $b, c \in B$, alors $n(sb, c) = n(s, c\overline{b}) = 0$. Cela montre que $sB \subset B^{\perp}$. En particulier, $B \cap sB = 0$. On a aussi $t(sb) = (sb) + \overline{(sb)} = n(sb, 1) = 0$ ce qui implique que $sb = -\overline{b}\overline{s}$, donc $\overline{s} = -s$ et $sb = \overline{b}s$. De plus, $s^2 = -s\overline{s} = -n(s) = \zeta$. Donc en utilisant le Lemme 1, on a que

$C = B \bigoplus sB$ est isomorphe à $CD(B, \zeta)$ comme algèbre avec involution. On peut maintenant déterminer la structure de A. Si $u \notin K$, alors $u^2 - t(u)u + n'u) = u^2 - u(u + \overline{u}) + u\overline{u} = 0$, ce qui montre que K[u] est isomorphe comme algèbre avec involution à l'extension quadratique K[x]/(m(x)) pour le polynôme $m(x) = x^2 - t(u)x + n(u)$. Le discriminant de m(x) est $\delta = ((t(u))^2 - 4n(u)$. Comme K n'est pas de caractéristique 2, $n(1,1) = 2 \neq 0$ donc n n'est pas dégénérée sur K et $K^{\perp}$. Dans ce cas, on peut prendre n'importe quel $u \in K^{\perp}$ avec $n(u) \neq 0$ pour avoir $\delta = -4n(u) \neq 0$.
Maintenant, si A=K[u], on peut s'arrêter là, sinon, on prends B=K[u], alors Q=C est une algèbre de quaternions. Sinon, on prends B=Q, et $\mathbb{O} = C$ est une algèbre d'octonions, sinon, on prends B=$\mathbb{O}$, et $C \subset A$ n'est pas alternée, ce qui est impossible, on a bien le résultat voulu.

13.1.3 Preuve du théorème

Soit R un anneau alterné à division non associatif, son centre K=C(R) est un corps, et on peut voir R comme une algèbre sur K. De plus, si R était commutatif, on aurait $3[a, b, c] = [a, b, c]^2 = 0$. et R serait associative, donc R n'est pas commutative. On pose $A_{a,b}(c) = [a, b, c]$, on a par les identités du Lemme 1 de la section précédente :

$$L_a A_{a,b} = Aa, ba \tag{1}$$

$$A_{a,b}(xy) = A_{a,b}(x)y + xA_{a,b}(y) - [[a, b], xy] \tag{2}$$

$$A^2_{a,b} = L_{[a,b]} A_{a,b} \tag{3}$$

On pose $B_{a,b} = L_{[a,b]} - A_{a,b}$, on peut réécrire (2) comme

$$B_{a,b}(xy) = B_{a,b}(x)y - xA_{a,b}(y). \tag{4}$$

On suppose que $A_{a,b} = 0$, en utilisant (2), on voit que $[a, b] \in N = N(R)$. Comme $A_{a,ba} = 0$ par (1) ,on a $[a, ba] \in N$. Si $[a, b] \neq 0, a = [a, b]^{-1}[a, ba] \in N$. Alors

$$A_{a,b} = 0 => [a, b] = 0 \, ou \, a \in N \tag{5}$$

Soit $b \in N, donc A_{a,b} = 0$ pour tout a$\in R$. Si $a \notin N$, on a clairement [a,b]=0. Si $a \in N$, il y a un certain $c \notin N$ car R n'est pas associative. Comme $c, a+c \notin N$, on a[a,b]=[a+c,b]-[c,b]=0. On a montre que $b \in N$ implique [a,b]=0 pour tout $a \in R$,c-a-d

$$N(R) = C(R) = K \tag{6}$$

$$A_{a,b} = 0 => [a, b] = 0 \tag{7}$$

On affirme maintenant que $\mathbb{A}_{a,b} = ker(A_{a,b})$ est une sous-algebre de R. Si [a,b]=0, c'est immediat de (2). Si$[a,b] \neq$ 0, on peut montrer encore plus.On pose $\mathbb{B}_{a,b} = ker(B_{a,b})$. Si $[a,b] \neq 0$, on affirme

$$R = \mathbb{A}_{a,b} \bigoplus \mathbb{B}_{a,b} \tag{8}$$

$$\mathbb{A}_{a,b} = Im\mathbb{B}_{a,b} \neq 0 \tag{9}$$

$$\mathbb{B}_{a,b} = Im\mathbb{A}_{a,b} \neq 0 \tag{10}$$

$$\forall a, b \in \mathbb{A}_{a,b},\ a+b \in \mathbb{A}_{a,b}\, et\, ab \in \mathbb{A}_{a,b} \tag{11}$$

C'est à dire $\mathbb{A}_{a,b}$est une sous-algebre de R

$$\tag{12}$$

$$\mathbb{B}_{a,b}\mathbb{A}_{a,b} + \mathbb{A}_{a,b}\mathbb{B}_{a,b} \subset \mathbb{B}_{a,b} \tag{13}$$

$$\mathbb{B}_{a,b}\mathbb{B}_{a,b} \subset \mathbb{A}_{a,b} \tag{14}$$

$$v\mathbb{A}_{a,b} = \mathbb{B}_{a,b}\, pour\, 0 \neq v \in \mathbb{B}_{a,b} \tag{15}$$

$$u \in N(\mathbb{A}_{a,b}), 0 \neq v \in \mathbb{B}_{a,b},\, avec\, [u, v, \mathbb{A}_{a,b}] = 0 => u \in K \tag{16}$$

Comme $A_{a,b}([a,b]) = (a,b,[a,b]) = 0$ par le lemme d'Artin, on remplace x par [a,b] dans (2), et cela montre que $A_{a,b}$ et $L_{[a,b]}$ commutent. Alors, $P = L^{-1}_{[a,b]}A_{a,b}$ vérifie $P^2 = P$ par (3). Alors $R = im(P) \bigoplus im(Id - P)$. On remarque que $Id - P = L^{-1}_{[a,b]}B_{a,b} = B_{a,b}L^{-1}_{[a,b]}$, donc

$$\mathbb{A}_{a,b} = ker(P) = im(Id - P) = im(\mathbb{B}_{a,b})$$
$$\mathbb{B}_{a,b} = ker(Id - P) = im(P) = im(\mathbb{A}_{a,b})$$

Comme $0 \neq a \in \mathbb{A}_{a,b}$ et $\mathbb{A}_{a,b} \neq R$ par (7), on déduit (8),(9,)(10).
Si $z, y \in \mathbb{A}_{a,b}$, on peut écrire $z = \mathbb{B}_{a,b}(x)$ et utiliser (4) pour obtenir $zy = \mathbb{B}_{a,b}(xy) \in \mathbb{A}_{a,b}$. Alors $\mathbb{A}_{a,b}$ est une sous-algèbre. Si $0 \neq x \in \mathbb{A}_{a,b}$, alors $y = x^{-1}$ dans (2) donne $0 = xA_{a,b}(x^{-1})$, donc $A_{a,b}(x^{-1}) = 0$ et $x^{-1} \in \mathbb{A}_{a,b}$ et on a (11). Soient $x \in \mathbb{B}_{a,b}$ et $y \in \mathbb{A}_{a,b}$, on utilises (4), on a $xy \in \mathbb{B}_{a,b}$, alors $\mathbb{B}_{a,b}\mathbb{A}_{a,b} \subset \mathbb{B}_{a,b}$, on a l'autre inclusion en passant dans l'algèbre opposée, et alors on a (12).
Pour montrer (13), on prends $x, z \in \mathbb{B}_{a,b}$ avec $z = A_{a,b}(y)$, on applique (6) pour obtenir $xz = -B_{a,b}(xy) \in \mathbb{A}_{a,b}$. Si $0 \neq v \in \mathbb{B}_{a,b}$ et $x \in \mathbb{B}_{a,b}$, soit $L_v^{-1}(x) = y + z$ avec $y \in \mathbb{A}_{a,b}$ et $z \in \mathbb{B}_{a,b}$. Comme x=vy+vz avec $vy \in \mathbb{B}_{a,b}$ et $vz \in \mathbb{A}_{a,b}$, on a vz=0, ce qui montre (14).
Finalement, pour (15), si $w \in \mathbb{A}_{a,b}$, alors [u,w,v]=-[u,v,w]=0. Comme $u \in N(\mathbb{A}_{a,b})$, la sous-algèbre $\mathbb{A}_{u,w}$ contient $\mathbb{A}_{a,b}$ et v. Alors,

$$R = \mathbb{A}_{a,b} \bigoplus v\mathbb{A}_{a,b} \subset \mathbb{A}_{u,w}$$

pour tout $w \in \mathbb{A}_{a,b}$. Alors, $[u, R, \mathbb{A}_{a,b}] = [u, \mathbb{A}_{a,b}, R] = 0$. Maintenant si $0 \neq z \in \mathbb{B}_{a,b}$, la sous-algèbre $\mathbb{A}_{u,z}$ contient $\mathbb{A}_{a,b}$ et z. Comme avant, cela montre $R \subset \mathbb{A}_{u,z}$, donc $[u, \mathbb{B}_{a,b}, R] = 0$. Alors, [u,R,R]=0, c-à-d $u \in N(R) = K$.
Comme R n'est pas commutatif, nous avons un $[p,q] \neq 0$. De plus,

$$[p,q]^{-1}[p,qp] = p \notin K,$$

donc [p,q] ou [p,qp] n'est pas dans K, quitte à remplacer q par qp si nécessaire, on peut supposer $r = [p, q] \notin K$. On pose $\mathbb{A} = \mathbb{A}_{p,q}$ et$\mathbb{B} = \mathbb{B}_{p,q}$. Clairement, $p, q \in \mathbb{A}$ et $r \in N(\mathbb{A})$ par (6). Comme $A_{p,q} = L_r P$ et $B_{p,q} = L_r(Id - P)$ où P est la projection sur $\mathbb{B}$, on obtient avec (12) et (4) avec $x \in \mathbb{A}$ et $y \in \mathbb{B}$:

$$\begin{aligned} 0 &= L_r(x)y - xL_r(y) \\ &= [r, x]y + [x, r, y] \end{aligned}$$

Si $r \in C(\mathbb{A})$, alors $[r, y, \mathbb{A}] = 0$ et $r \in K$ par (15), et on a une contradiction. Cela montre que $N(\mathbb{A} \neq C(A)$. Par (6), on voit que $\mathbb{A}$ n'est pas strictement alternative, c-à-d que $\mathbb{A}$ est associative.
Si $0 \neq s \in \mathbb{B}$, alors $s^2 \in \mathbb{A} = N(\mathbb{A})$ et $[s^2, s, R] = 0$ par le lemme d'Artin. Alors (15) montrer que $\zeta = s^2 \in K$. Alors $s^{-1} = \zeta^{-1}s$ est un élément de la sous-algèbre associative engendrée par s et $a \in R$. On va montrer que $j : a- > \overline{a} = sas^{-1}$ est une K-involution de $\mathbb{A}$. D'abord, on remarque que $\overline{\overline{a}} = \zeta a \zeta^{-1} = a$. On a aussi

$$a\overline{a} = asa\zeta^{-1}s = \zeta^{-1}(as)^2 \in K$$

La linéarisation donne $a\overline{b} + b\overline{a} \in K$ et $a + \overline{a} \in K$ pour $a, b \in \mathbb{A}$. Alors, $[\overline{a}, x, y] + [a, x, y] = 0$ pour tout $x, y \in R$. Si $a, b \in \mathbb{A}$, alors

$$\begin{aligned} a(sb) &= (as)b - [a, s, b] \\ &= (s\overline{a})b - [s, \overline{a}, b] \\ &= s(\overline{a}b) \end{aligned}$$

On a maintenant

$$\begin{aligned} (aba)s &= a(b(as)) = a(b(s\overline{a})) \\ &= a(s(\overline{b}\overline{a})) \\ &= s(\overline{a}\overline{b}\overline{a}) \end{aligned}$$

Alors j vérifie $\overline{aba} = \overline{a}\overline{b}\overline{a}$. On pose alors

$$p(x, y, z) = (z - xy)(z - yx)$$

On a pour $a, b, c \in \mathbb{A}$, $\overline{p(a, b, c)} = p(\overline{a}, \overline{b}, \overline{c})$. Si on prends c=ab, on obtient :

$$0 = \overline{p(a, b, ab)} = p(\overline{a}, \overline{b}, \overline{ab}) = (\overline{ab} - \overline{a}\overline{b})(\overline{ab} - \overline{b}\overline{a})$$

On voit donc que pour toute paire $a, b \in \mathbb{A}$, on a au choix $\overline{ab} = \overline{a}\overline{b}$ ou $\overline{ab} = \overline{b}\overline{a}$. Si $\overline{ab} = \overline{a}\overline{b}$, alors

$$[\overline{a}, \overline{b}, s] = [a, b, s] = s(\overline{ab} - \overline{a}\overline{b}) = 0$$

Comme $\mathbb{A}$ est associative, la sous-algèbre $\mathbb{A}_{\overline{a},\overline{b}}$ contient $\mathbb{A}$ et s donc contient R. On remarque que $A_{\overline{a},\overline{b}} = 0$ et que $[\overline{a}, \overline{b}] = 0$ par (7). Alors $\overline{ab} = \overline{b}\overline{a}$ dans tous les cas, donc j est une K-involution.

Comme $r = [p, q] \neq 0$, on a que $\mathbb{A}$ n'est pas commutative et que j n'est pas l'identité. D'un autre coté, si $t(\mathbb{A}) = 0$, alors 2=t(1)=0 et $\overline{a} = -a = a$ pour $a \in \mathbb{A}$. Comme j n'est ps l'identité, il existe un $u \in \mathbb{A}$, tel que $t(u) \neq 0$. On peut maintenant montrer que la "norme" forme quadratique $n(a) = a\overline{a}$ sur $\mathbb{A}$ est non dégénérée. En effet, si $0 \neq a \in \mathbb{A}$, soit $b = \overline{a^{-1}u}$. On a

$$n(b, a) = b\overline{a} + a\overline{b} = t(a\overline{b}) = t(u) \neq 0$$

qui est ce qu'on voulait montrer. On peut désormais appliquer le lemme 2, ce qui montre que $\mathbb{A}$ qui est associative mais non commutative est une algèbre de quaternions. Par le lemme 1, $R = \mathbb{A} \bigoplus s\mathbb{A} \cong CD(\mathbb{A}, \zeta)$ est une algèbre d'octonions.

Références

[1] E. Artin, Geometric Algebra, Interscience Publishers, New York-London, 1957

[2] R. Bruck et E.Kleinfeld, The structure of alternative division rings, Proc. Amer. Math. Soc. 2, (1951). 878-890

[3] P. Samuel, Géométrie projective, Presses Universitaires de France, Paris, 1986

[4] E. Shult, Points and lines. Characterizing the classical geometries. Universititext. Springer, Heidelberg, 2011

[5] C. Weibel, Survey if Non-Desarguesian Planes, Notices of the AMS, volume 54, number 10 (2007) 1294-1303

[6] M. Hall , The Theory of Groups , 434 pp., Macmillan, 1959

[7] Tsuzuku, Finite Groups and Finite Geometries