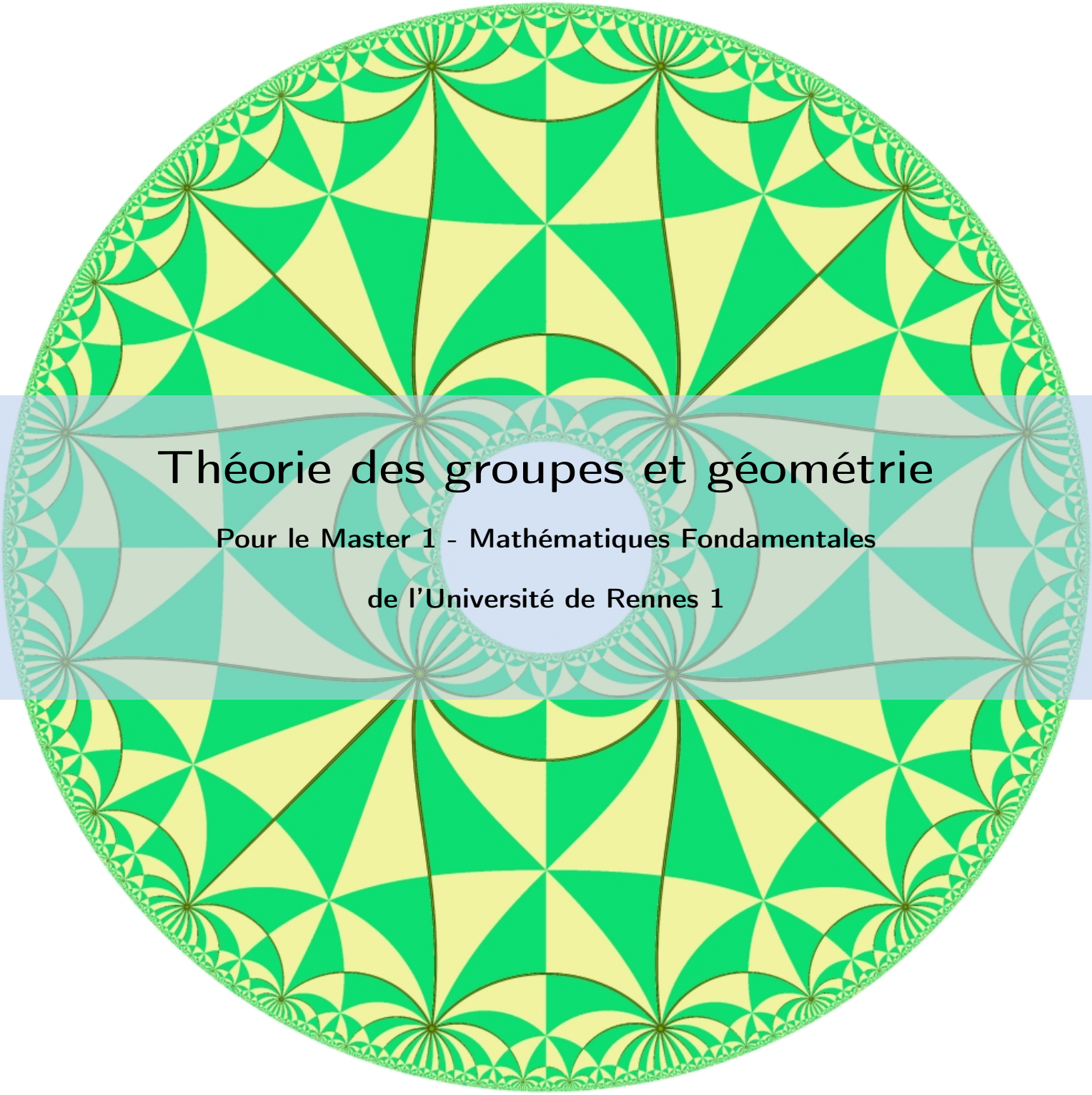

Théorie des groupes et géométrie

Pour le Master 1 - Mathématiques Fondamentales

de l'Université de Rennes 1

Le template utilisé pour le rendu du polycopié est le Legrand Orange Book disponible sur le web à l'adresse suivante :
https://www.latextemplates.com/template/the-legrand-orange-book

Table des matières

Déroulement du cours, emploi du temps

Présentation

- Bureau 309
- Mail : ludovic.marquis@univ-rennes1.fr
- Cours le vendredi 14h → 16h par Ludovic Marquis.
- Il y a 2 groupes :
  - TD groupe magistère à Ker Lann, le mardi 8h → 10h, encadré par Salim Rostam.
  - TD groupe Beaulieu à Beaulieu, le mardi à 8h → 10h, encadré par Ludovic Marquis.
- Page oueb avec un résumé, les TD (au fur et à mesure).
  - `https://perso.univ-rennes1.fr/ludovic.marquis`
  - accessible en tapant ludovic marquis dans votre moteur de recherche préféré.
  - cliquer Enseignement.
  - cliquer THGG.
- Evaluation
  - Deux contrôles de 2 heures, un en milieu de semestre et un à la fin. Amener vos feuilles !! $\rightsquigarrow C1$ et $C2$
  - $F = \frac{C1+C2}{2}$.
  - Si vous êtes ABI à l'épreuve i alors $C_i = 0$.
  - Si vous êtes ABJ à une ou deux épreuves alors il vous sera proposé une épreuve de substitution.
  - Attention : il n'y a pas de rattrapage !
  - Toutes les justifications d'absence doivent être envoyées à Annie Quéméré.
- 1/3-temps !!!

Biblio

1. **Le Perrin**, Cours d'Algèbre, Daniel Perrin, Ellipses.
2. **Le Audin**, Géométrie, Michel Audin, EDP Sciences.
3. **Le Delcourt**, Théorie des groupes, Jean Delcourt, Dunod.

4. Deux autres sur la page oueb pour les plus motivés.

Syllabus

1. Rappels sur les groupes et les actions de groupes. Résolubilité, simplicité.
2. Groupes symétriques et alternés, familles de générateurs, résolubilité.
3. Groupe linéaire, spécial linéaire sur un corps. Familles de générateurs, résolubilité. Drapeaux, décomposition LU, décomposition de Bruhat.
4. Groupes linéaires sur un corps fini, utilisation des inversibles d'une sous-algèbre de matrices pour trouver des sous-groupes de Sylow.
5. Géométrie projective : définitions, structure affine du complémentaire d'un hyperplan, homographies, théorèmes de Thalès, Pappus, Desargues. Dualité.
6. Formes sesquilinéaires et quadratiques : réduction. groupes orthogonaux et symplectiques. Théorème de Witt. Théorème de Cartan-Dieudonné.
7. Formes quadratiques sur $\mathbb{R}$. Compacité du groupe orthogonal, sous-groupes fermés (théorème de Cartan) et compacts du groupe linéaire, sous-groupes finis de SO_3, polyèdres réguliers. Décompositions de Cartan et d'Iwasawa.

Prérequis

Le cours de Théorie des groupes de la licence 3 de mathématiques pour la recherche, dont le syllabus est :

1. Groupes, sous-groupes, théorème de Lagrange, ordre d'un élément. Exemple du groupe diédral.
2. Homomorphismes et isomorphismes de groupes ; propriété universelle du groupe $(\mathbb{Z}, +)$.
3. Sous-groupes distingués, groupes quotients, propriété universelle du quotient. Exemples $(\mathbb{Z}/n\mathbb{Z})$. Correspondance entre sous-groupes d'un groupe et d'un de ses quotients.
4. Produits de groupes : groupe produit de sous-groupes. Produits semi-directs.
5. Groupes cycliques : générateurs, sous-groupes, groupe multiplicatif d'un corps fini.
6. Groupe symétrique. Conjugué dune permutation, décomposition en cycles disjoints, signature. Groupe alterné.
7. Actions de groupe : orbites, stabilisateurs, formule des classes, formule de Burnside, exemples (groupe agissant sur lui-même ou sur ses parties par translation, par conjugaison), applications (sous-groupe d'indice p minimal, théorème de Burnisde, sous-groupes finis de SO_3, nombre d'orbites).
8. Théorèmes de Cauchy et de Sylow. Applications : classification des groupes d'ordre 12, 30, etc. Groupes définis par générateurs et relations.
9. Groupes abéliens de type fini.

Techniquement, B.C. :

1. a fait “seulement” : le produit semi-direct interne.
2. n'a pas fait : sous-groupes finis de SO_3.
3. n'a pas fait : Groupes définis par générateurs et relations.

1. Les bases de la théorie des groupes

I Exemples importants de groupes

Les exemples de groupes les plus importants sont données par (dans le désordre) : $\mathbb{Z}$, $\mathbb{Z}^d$, $\mathbb{Z}/n\mathbb{Z}$, le groupe $\mathfrak{S}(X)$ des bijections d'un ensemble X, le groupe $\mathrm{GL}(V)$ des automorphismes linéaires d'un espace vectoriel V et leurs sous-groupes.

Le but de ce cours est de "comprendre" les groupes en les faisant agir sur des espaces appropriés, et inversement de comprendre les propriétés de certains espaces géométriques à l'aide d'action de groupes.

II Actions de groupes

1. C'est quoi ?

Définition II.1 Une *action d'un groupe G sur un ensemble X* est la donnée équivalente d'un morphisme $\varphi : G \to \mathfrak{S}(X) = \mathrm{Bij}(X)$ ou d'une application $\Phi : G \times X \to X, (g,x) \mapsto \Phi(g,x) = g \cdot x$, qui vérifie :

- $\forall x \in X, \Phi(e,x) = e \cdot x = x$.
- $\forall g,h \in G, \forall x \in X, \Phi(g,\Phi(h,x)) = g \cdot (h \cdot x) = (gh) \cdot x = \Phi(gh,x)$.

On notera : $G \curvearrowright X$ [a].

a. C'est une notation courante sans être pour autant universelle

Démonstration. L'équivalence entre les deux points de vue se voient via l'égalité : $\varphi(g)(x) = \Phi(g,x)$. ∎

Définition II.2 Soit $x \in X$, l'ensemble :

$$\mathcal{O}_x = \{y \in X \mid \exists g \in G, g \cdot x = y\}$$

s'appelle *l'orbite de x sous G*.

Définition II.3 La relation binaire $\mathcal{R}$ sur l'ensemble X définie par :

$$x\mathcal{R}y \quad \Leftrightarrow \quad \exists g \in G, g \cdot x = y$$

est une relation d'équivalence, dont les classes d'équivalences sont les orbites de l'action de G sur X. Par conséquent, deux orbites sont égales ou disjointes. Les orbites forment une partition de X. L'ensemble des orbites est noté X/G.

2. Formules des classes

On obtient la première formule des classes :

Proposition II.1 — Première formule des classes. Soit G un groupe agissant sur un ensemble fini X. On a :

$$\#X = \sum_{\mathcal{O} \in X/G} \#\mathcal{O} = \sum_{i=1}^{n} \#\mathcal{O}_{x_i}$$

où $\{x_1, ..., x_n\}$ est une *transversale* (ou un *ensemble de représentants*) de $\mathcal{R}$ i.e. un sous-ensemble de X qui rencontre en un et un seul élément toutes les classes d'équivalences de $\mathcal{R}$.

Définition II.4 Soit $G \curvearrowright X$. Soit $x \in X$, on note Stab_x le sous-groupe de G des éléments de G qui fixe x :

$$\mathrm{Stab}_x = \{g \in G \,|\, g \cdot x = x\}$$

On l'appelle le *stabilisateur de* x.

L'application orbitale $\varphi_x : G \to X$, $g \mapsto g \cdot x$ a pour image l'orbite de x. Deux éléments g, h ont la même image par φ_x si et seulement si $g^{-1}h \in \mathrm{Stab}_x$. Ainsi, φ_x induit une bijection :

$$\varphi_x : G/\mathrm{Stab}_x \to \mathcal{O}_x, g \mapsto g \cdot x$$

On en déduit la seconde formule des classes :

Proposition II.2 — Seconde formule des classes. Soit $G \curvearrowright X$. On suppose G et X fini. Pour tout $x \in X$, on a :

$$\#\mathcal{O}_x \cdot \#\mathrm{Stab}_x = \#G$$

Enfin, on peut démontrer le Lemme de Burnside :

Lemma II.3 — Lemme de Burnside. Soit $G \curvearrowright X$. On suppose G et X fini. On a :

$$\#X/G = \frac{1}{\#G} \sum_{g \in G} \#\mathrm{Fix}(g) = \frac{1}{\#G} \sum_{x \in X} \#\mathrm{Stab}_x$$

où $\mathrm{Fix}(g)$ est l'ensemble des points fixes de g, i.e. $\mathrm{Fix}(g) = \{x \in X \,|\, g \cdot x = x\}$.

Démonstration. On décrit un même ensemble de deux façons différentes :

$$\begin{aligned} \{(g,x) \,|\, g \cdot x = x\} &= \{(g,x) \,|\, g \in G, x \in \mathrm{Fix}(g)\} \\ &= \{(g,x) \,|\, x \in X, g \in \mathrm{Stab}_x\} \end{aligned}$$

On obtient donc que :

$$\sum_{g\in G} \#\mathrm{Fix}(g) = \sum_{x\in X} \#\mathrm{Stab}_x$$

Les orbites forment une partition de X, on a donc :

$$\sum_{x\in X} \#\mathrm{Stab}_x = \sum_{\mathcal{O}\in X/G} \underbrace{\sum_{x\in\mathcal{O}} \#\mathrm{Stab}_x}_{=\#G}$$

Mais, deux éléments d'une même orbite ont des stabilisateurs conjugués [1] donc de même ordre, on obtient donc pour tout $y \in X$:

$$\sum_{x\in\mathcal{O}_y} \#\mathrm{Stab}_x = \#\mathcal{O}_y \#\mathrm{Stab}_y = \#G$$

Finalement, on a obtenu :

$$\sum_{x\in X} \#\mathrm{Stab}_x = \sum_{\mathcal{O}\in X/G} \#G = \#X/G\#G$$

D'où le résultat. ■

R En particulier, cette formule dit que le nombre d'orbites est la moyenne du nombre de points fixes des éléments de G.

3. Vocabulaire

Définition II.5 L'action $G \curvearrowright X$ est dite :

- *fidèle* si le morphisme $\varphi : G \to \mathfrak{S}(X)$ est injectif. Autrement dit, si tous les éléments de G agissent de façon non-trivial. Le *noyau de l'action* $G \curvearrowright X$, noté $\ker(G \curvearrowright X)$ est le noyau de $\varphi : G \to \mathfrak{S}(X)$.
- *libre* lorsque tous les stablisateurs sont triviaux. Autrement dit, lorsque : $\forall x \in X,\ \forall g \in G,\quad g\cdot x = x \Rightarrow g = e$.
- *transitive* lorsque qu'il n y'a qu'une seule orbite, i.e. $\forall x, y \in X,\ \exists g \in G$, tel que $y = g\cdot x$.
- *simplement transitive* lorsqu'elle est libre et transitive, i.e. $\forall x, y \in X,\ \exists! g \in G$, tel que $y = g\cdot x$.
- *k-transitive* lorsque l'action de G sur X^{*k} est transitive, où X^{*k} est l'ensemble des k-uplet d'éléments distincts.
- *simplement k-transitive* lorsque l'action de G sur X^{*k} est simplement transitive.

4. Exemples

Action par translation et actions induites sur les quotients

Tout groupe agit sur lui-même par translation à gauche : $G \times G \to G,\ (g,x) \mapsto gx$.

R Cette action est fidèle et simplement transitive.

1. Rappel : $\mathrm{Stab}_{gx} = g\mathrm{Stab}_x g^{-1}$

Corollaire II.4 Tout groupe d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Si H est un sous-groupe de G, alors on peut faire agir G par multiplication à gauche sur G/H l'ensemble des classes à droite de G modulo H : $G \times G/H \to G/H$, $(g, xH) \mapsto gxH$.

Action par conjugaison et par automorphisme, et l'action induite sur l'ensemble des sous-groupes

Tout groupe agit sur lui-même par conjugaison : $G \times G \to G$, $(g,x) \mapsto gxg^{-1}$.

R

- Les orbites de cette action s'appelle les *classes de conjugaison* de G.
- Le noyau de cette action est le *centre* $\mathcal{Z}(G)$ de G, c'est à dire :

$$\mathcal{Z}(G) = \{x \in G \,|\, gx = xg,\ \forall g \in G\}$$

Le groupe $\mathrm{Aut}(G)$ des automorphismes de G agit sur G : $\mathrm{Aut}(G) \times G \to G$, $(\varphi, x) \mapsto \varphi(x)$.

R L'action par conjugaison de G sur lui-même induit un morphisme de $G \to \mathrm{Aut}(G)$ dont le noyau est le centre de G. L'image de ce morphisme s'appelle le groupe des *automorphismes intérieurs* de G.

Ces deux actions induisent des actions sur l'ensemble des sous-groupes de G.

R

- Un sous-groupe H de G est fixé par G sous l'action par conjugaison lorsque :

$$\forall g \in G, gHg^{-1} = H$$

  Autrement dit, H est *distingué / normal*.
- Un sous-groupe H de G fixé par $\mathrm{Aut}(G)$ sous l'action par automorphisme est dit *caractéristique*.
- Le stablisateur de H dans G pour l'action par conjugaison s'appelle le *normalisateur* de H, on le note $N_G(H)$. Autrement dit, on a :

$$N_G(H) = \{g \in G \,|\, gHg^{-1} = H\}$$

- Le sous-groupe de G qui fixe tous les éléments de H s'appelle le *centralisateur* de H, on le note $Z_G(H)$. Autrement dit, on a :

$$Z_G(H) = \{g \in G \,|\, \forall h \in H, ghg^{-1} = h\}$$

Représentation linéaire

Une *représentation linéaire* d'un groupe G dans $\mathrm{GL}(V)$ où V est un k-espace vectoriel. Il s'agit donc d'une action du groupe G par transformation linéaire sur l'espace vectoriel V.

Par exemple, à toute action d'un groupe G sur un ensemble fini X, on peut associer une représentation ρ sur l'espace vectoriel k^X des fonctions de $X \to k$ via la formule : $g \cdot f(x) = f(g^{-1}x)$. Si on veut écrire cette action dans la base $(e_x)_{x \in X}$, il suffit d'observer que $g \cdot e_x = e_{g \cdot x}$.

Des actions plus géométriques

- L'action du groupe linéaire $\mathrm{GL}_n(\mathbb{R})$, du groupe affine $\mathrm{GA}_n(\mathbb{R})$ ou du groupe des isométries affines euclidiennes $\mathrm{Isom}(\mathbb{R}^n)$ sur $\mathbb{R}^n$.

- Le groupe affine de k^n est donné par les transformations de k^n de la forme $T_{A,B} : x \mapsto Ax + b$ où $A \in \mathrm{GL}_n(k)$ et $B \in k^n$. On peut aussi voir ce groupe comme l'ensemble des matrices de $\mathrm{GL}_{n+1}(k)$ de la forme :

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

- L'action du groupe orthogonal $\mathrm{O}_n(\mathbb{R})$ sur la sphère unité $\mathbb{S}^{n-1}$ de $\mathbb{R}^n$.
- On découvrira un nouvel espace : l'espace projectif $k\mathbb{P}^n$ sur lequel agira le groupe $\mathrm{PGL}_{n+1}(k) = \mathrm{GL}_{n+1}(k)/Z$.
- ...

III Théorèmes de Lagrange, Cauchy et Sylow

On rappelle sans démonstration les théorèmes de Lagrange, Cauchy et Sylow.

1. Théorème de Lagrange

Théorème III.1 — Théorème de Lagrange. L'ordre d'un sous-groupe divise l'ordre du groupe.

Démonstration. On fait agir H sur G par translation à gauche. Cette action est libre. On applique la seconde formule des classes. ■

2. Théorème de Cauchy

Théorème III.2 — Théorème de Cauchy. Soit G un groupe fini et p un nombre premier qui divise l'ordre de G. Il existe un élément d'ordre p dans G.

Démonstration. On introduit l'ensemble suivant :

$$X = \{(x_1, \ldots, x_p) \in G^p \mid x_1 \cdots x_p = 1\}$$

On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X par permutation circulaire. Par la seconde formule des classes, une orbite est de cardinal 1 ou p. Les orbites de cardinal 1 correspondent aux éléments de X qui vérifient :

$$x_1 = x_2 = \cdots = x_p$$

Autrement dit, chaque orbite de cardinal 1 fournit une solution à l'équation :

$$x^p = 1$$

On note k_1 le nombre d'orbites de cardinal 1 et k_p le nombre d'orbites de cardinal p. Par la première formule des classes, on a :

$$\#X = 1 \cdot k_1 + p \cdot k_p$$

Or, $\#X = n^{p-1}$. Par conséquent, p divise k_1 mais $k_1 \geqslant 1$ puisque $(e, \ldots, e)$ fournit une orbite de cardinal 1. ■

3. Théorème de Sylow

L'énoncé

Théorème III.3 — Théorème de Sylow. Soit G un groupe fini d'ordre $p^\alpha m$ avec $p \wedge m = 1$ où p est un nombre premier. On note s_p le nombre de p-Sylow de G. Alors

1. $s_p \geqslant 1$.
2. Tout sous-groupe de G d'ordre une puissance de p est inclus dans un p-Sylow de G.
3. Le groupe G agit transitivement sur l'ensemble de ses p-Sylow par conjugaison.
4. $s_p \equiv 1\,[p]$ et $s_p | m$.

R Si $s_p = 1$ alors le p-Sylow de G est unique et donc distingué.

Un exemple à retenir

Notation : Soit p un nombre premier. On note $\mathbb{F}_p$ le corps $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$. C'est l'unique corps de cardinal p.

Lemma III.4 Le sous-groupe $\mathrm{U}_n(\mathbb{F}_p)$ des matrices triangulaires supérieures de diagonale 1 est un p-Sylow du groupe $\mathrm{GL}_n(\mathbb{F}_p)$.

Démonstration. Le cardinal du groupe $\mathrm{GL}_n(\mathbb{F}_p)$ est :

$$(p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1}) = 1\cdot p\cdot p^2\cdots p^{n-1}\cdot m \qquad = p^{\frac{n(n-1)}{2}} m$$

Le cardinal de $U_n(\mathbb{F}_p)$ est $p^{\frac{n(n-1)}{2}}$. ∎

IV Simplicité

1. C'est quoi ?

Définition IV.1 Un groupe G est dit *simple* lorsque tout sous-groupe distingué est trivial ou G tout entier.

▪ **Exemple 1.1** Voici la liste des groupes simples que l'on croisera dans ce cours. Seule la première affirmation est facile à démontrer.

- Les groupes cycliques $\mathbb{Z}/p\mathbb{Z}$ d'ordre premier.
- Les groupes alternés $\mathfrak{A}_n$ pour $n \geqslant 5$.
- Les groupes linéaires $\mathrm{PSL}_n(k)$ pour $n \geqslant 2$ et k quelconque sauf si $(n,k) = (2,\mathbb{F}_2)$ et $(2,\mathbb{F}_3)$. Voir Chapitre 3.
- Les groupes orthogonaux $\mathrm{PSO}_n(\mathbb{R})$ pour $n = 3$ ou $n \geqslant 5$. Voir Chapitre ?.

▪

2. Application des théorèmes de Sylow à la non-simplicité

Exercice 1.1 En utilisant le Théorème de Sylow, montrer qu'un groupe d'ordre pq^α avec p, q premiers, $\alpha \geqslant 1$ et $p < q$ n'est jamais simple. *Le théorème de Sylow affirme que $s_q | p$ et $s_q = 1 + kq$ donc $k = 0$ puisque $p < q$. Ainsi $s_q = 1$ et le q-Sylow de G est distingué.* Idem avec $p^2 q \neq 12$. ▪

.....Fin du cours 1.....

V Groupe dérivé

Définition V.1 Soit G un groupe. Le *groupe dérivé* de G est le sous-groupe de G engendré par tous les *commutateurs* $[x,y]=xyx^{-1}y^{-1}$ de G. On le note $D(G)$ ou G'.

Proposition V.1 Le groupe dérivé est un sous-groupe distingué de G même caractéristique.

Démonstration. Soit α un automorphisme de G, on a $\alpha([x,y])=[\alpha(x),\alpha(y)]$... ■

Proposition V.2 Soit G un groupe.

- Le groupe dérivé de G est trivial si et seulement si G est abélien.
- Le groupe quotient $G/D(G)$ est abélien.
- Soit A un groupe abélien et $\varphi : G \to A$ un morphisme. Alors $D(G) \subset \ker(\varphi)$, ainsi le morphisme $\varphi : G \to A$ se factorise par la projection canonique $G \to G/D(G)$.
- Si G/H est abélien alors $D(G) \leqslant H$.
- Le groupe $G/D(G)$ s'appelle *l'abélianisé de* G, c'est le plus grand quotient abélien de G.

Démo en exo. Le premier point est trivial. Le second point se vérifie par soient $x,y \in G$, calculons le commutateur $[\bar{x},\bar{y}] \in G/D(G)$, on a : $[\bar{x},\bar{y}]=[\bar{x,y}]=1$. Le troisième point est une conséquence du fait que l'image d'un commutateur est trivial. Le quatrième point est une application du troisième avec $A=G/H$ et $\varphi : G \to G/H$ la projection canonique. ■

Définition V.2 On définit les groupes dérivés d'ordre supérieur de la façon suivante :

- $D^{(0)}(G)=G^{(0)}=G$.
- $D^{(k+1)}(G)=G^{(k+1)}=D(D^{(k)}(G))$.

La suite $(D^{(k)}(G))_{k\in\mathbb{N}}$ s'appelle la *suite dérivée* de G.

VI Classification des groupes abéliens de type fini

Définition VI.1 Un groupe est dit de *type fini* lorsqu'il est engendré par un nombre fini d'éléments.

Théorème VI.1 — Classification des groupes abéliens de type fini. Soit Γ un groupe abélien de type fini alors :

1. Il existe un unique entier $l \geqslant 0$ et un n-uplet $(q_1,\dots,q_n)$ de puissances[a] de nombres premiers, unique à permutation près, tel que Γ est isomorphe au groupe :
$$\mathbb{Z}^l \times \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_n\mathbb{Z}$$
2. Il existe un unique entier $l \geqslant 0$ et un unique m-uplet $(a_1,\dots,a_m)$ d'entiers >1, qui vérifie $a_m | a_{m-1} | \cdots | a_1$ tel que Γ est isomorphe au groupe :
$$\mathbb{Z}^l \times \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_m\mathbb{Z}$$

a. non triviales...

R On passe d'un point de vue à l'autre en utilisant le théorème chinois : Les groupes $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ sont isomorphes si et seulement si m et n sont premiers entre eux.

▪ **Exemple 1.2** Ce théorème permet de lister les groupes finis abéliens d'ordre n fixé, à isomorphisme près, par exemple :

1. La liste des groupes finis abéliens d'ordre $8 = 2^3$ est :

$$\mathbb{Z}/8\mathbb{Z} \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad (\mathbb{Z}/2\mathbb{Z})^3$$

c.à.d. $n = 1, q_1 = 8$, puis $n = 2, q_1 = 4$ et $q_2 = 2$, et enfin $n = 3$ et $q_1 = q_2 = q_3 = 2$.

2. La liste des groupes finis abéliens d'ordre $24 = 2^3 \cdot 3$ est :

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \quad (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/3\mathbb{Z}$$

qui est égale à la liste :

$$\mathbb{Z}/24\mathbb{Z} \quad \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$$

c.à.d. $m = 1, a_1 = 24$, puis $m = 2, a_1 = 12$ et $a_2 = 2$ et enfin $m = 3, a_1 = 6, a_2 = a_3 = 2$.

▪

Exercice 1.2 Donner la liste des groupes abéliens d'ordre $2^3 \cdot 3^2$, recommencer avec un autre exemple, jusqu'à compréhension... ▪

Exercice 1.3 Obtenir une formule explicite pour A_n le nombre de groupes abéliens d'ordre n à isomorphisme près, en fonction de la décomposition en nombre premiers de n. On pourra commencer par calculer A_{p^α}, etc... ▪

VII Extension de groupes

On va parler dans cette section de produit semi-direct interne et externe, suite exacte et d'extension centrale.

1. Un petit lemme

Notation : Soient $H, K \leqslant G$. On note HK le sous-ensemble de G donnée par :

$$HK = \{hk \,|\, h \in H, k \in K\}$$

Proposition VII.1 Soient G un groupe et H, K deux sous-groupes de G. Si H ou K est distingué alors l'ensemble HK est un sous-groupe de G et $HK = KH$.

Démonstration. Supposons H distingué. On a $HK = KH$ car :

$$hk = k \underbrace{k^{-1} h k}_{\in H}$$

On en déduit que l'ensemble $HK = KH$ est stable par passage à l'inverse. Reste la stabilité par produit. Soient h, k, h', k' avec des notations évidentes.

$$hkh'k' = h \underbrace{(kh'k^{-1})}_{\in H} kk' \in HK$$

■

2. Produit semi-direct version interne

Définition VII.1 Soit G un groupe. Soient N et K deux sous-groupes de G, on dit que G est le *produit semi-direct (interne) de N par K* lorsque les 3 assertions suivantes sont vérifiées :

1. $N \lhd G$
2. $N \cap K = \{1\}$
3. $NK = G$

Dans ce cas, on note $G = N \rtimes K$.

Proposition VII.2 Si $G = N \rtimes K$ alors :

1. $\forall g \in G, \exists! (n,k) \in N \times K$, tel que $g = nk$.
2. $(nk)(n'k') = n(kn'k^{-1})kk'$
3. L'application $G \to K$ donnée par $nk \mapsto k$ est un morphisme surjectif de noyau N.

Démonstration. L'existence est donné par le troisième point. L'unicité vient du second. En effet, soient $n, n' \in N$ et $k, k' \in K$ tel que $nk = n'k'$. On a $n'^{-1}n = k'k^{-1} \in N \cap K$. Donc $n = n'$ et $k = k'$. Le second point est trivial, mais il montre grâce au premier, le troisième point. ■

Définition VII.2 Soit G un groupe. Soit N un sous-groupe distingué de G. On dit que N admet *un complément* lorsqu'il existe un sous-groupe K de G tel que :

1. $N \cap K = \{1\}$
2. $NK = G$

Proposition VII.3 Soit $G = N \rtimes K$. Le groupe K est distingué dans G si et seulement si K centralise N. Dans ce cas, on dit que le produit est *direct*, et on note $G = H \times K$.

Démonstration. Si K est distingué dans G alors pour tout $n \in N$ et tout $k \in K$, on a $[n,k] \in N \cap K$, d'où $[n,k] = 1$, ce qui veut dire que K centralise N. La réciproque est triviale. ■

Exemple VII.1 On donne une liste d'exemples de groupe distingué dans des groupes usuels et de complément (le complément n'est pas unique).

On définit quatre groupes :

$$\mathrm{GA}(k^d) = \left\{ \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \middle| A \in \mathrm{GL}_d(k), b \in k^d \right\} \leqslant \mathrm{GL}_{d+1}(k)$$

$$\mathrm{T}_n(k) = \begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix} \qquad \mathrm{U}_n(k) = \begin{pmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \mathrm{A}_n(k) = \begin{pmatrix} * & 0 & 0 & 0 \\ 0 & * & 0 & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \end{pmatrix}$$

Ou de façon plus formel :

- $\mathrm{T}_n(k) = \{M \in \mathrm{GL}_n(k) \,|\, M_{i,j} = 0, \forall i > j\}$
- $\mathrm{U}_n(k) = \{M \in \mathrm{T}_n(k) \,|\, M_{i,i} = 1, \forall i\}$
- $\mathrm{A}_n(k) = \{M \in \mathrm{GL}_n(k) \,|\, M_{i,j} = 0, \forall i \neq j\}$

Groupe G	Groupe distingué N	Complément K
Le groupe symétrique $\mathfrak{S}_n$	le groupe alterné $\mathfrak{A}_n$	un sous-groupe engendré par une transposition
Le groupe linéaire $\mathrm{GL}_n(k)$	le groupe spécial $\mathrm{SL}_n(k)$ linéaire	$\left\{\begin{pmatrix}\lambda & 0\\ 0 & \mathrm{Id}\end{pmatrix} \mid \lambda \in k^*\right\}$
Le groupe dihédral $\mathbb{D}_{2n}$, $\mathbb{D}_\infty$	Le sous-groupe des rotations $\simeq \mathbb{Z}/n\mathbb{Z}$	un sous-groupe engendré par une réflexion
$\mathrm{T}_n(k)$	$\mathrm{U}_n(k)$	$\mathrm{A}_n(k)$
Le groupe affine $\mathrm{GA}_n(k)$	Le groupe des translations $\simeq k^n$	Le groupe linéaire = Le stabilisateur de l'origine

3. Produit semi-direct externe

Définition VII.3 Soit G un groupe. On note $\mathrm{Aut}(G)$ le groupe des automorphismes de G.

Définition VII.4 Soient N, K deux groupes et $\alpha : K \to \mathrm{Aut}(N)$ un morphisme. On appelle *produit semi-direct (externe) de N par K relativement à α*, noté $N \rtimes_\alpha K$, le groupe G suivant :

1. En tant qu'ensemble $G = N \times K$.
2. Neutre $1 = (1_N, 1_K)$
3. Le produit est donné par :

$$(n,k) \bullet (n',k') = (n\alpha(k)\cdot n', kk') = ({}^k n', kk')$$

On (parfois) notera ${}^k n$ pour $\alpha(k)\cdot n$ pour se simplifier la vie.

Proposition VII.4 Soient N, K deux groupes et $\alpha : K \to \mathrm{Aut}(N)$ un morphisme.

1. Le couple $(N \rtimes_\alpha K, \bullet)$ est un groupe.
2. $N \times \{1_K\}$ est un sous-groupe distingué de $N \rtimes_\alpha K$.
3. L'application $N \to N \rtimes_\alpha K$, donnée par $n \mapsto (n, 1_K)$ est un morphisme injectif.
4. L'application $K \to N \rtimes_\alpha K$, donnée par $k \mapsto (1_N, k)$ est un morphisme injectif.
5. $\{1_N\} \times K$ est un sous-groupe de $N \rtimes_\alpha K$.
6. Le groupe $N \rtimes_\alpha K$ est le produit semi-direct interne de $N \times \{1_K\}$ par $\{1_N\} \times K$.
7. Si $n \in N$, $k \in K$ alors (avec les abus de notations nécessaires) on a $\alpha(k)\cdot n = knk^{-1}$.

Démonstration. Le premier point est une vérification un peu pénible laissé au lecteur en exercice. On remarque que la réunion de N et K engendrent G puisque : $(n,1_K)(1_H,k) = (n,k)$. Donc pour montrer que $N \times \{1_K\}$ est un sous-groupe distingué de $N \rtimes_\alpha K$, il suffit de montrer qu'il est normalisé par $\{1_H\} \times K$.

$$(1,k)(n,1)(1,k^{-1}) = (1,k)(n,k^{-1}) = ({}^k n, kk^{-1}) = ({}^k n, 1)$$

Ce qui montre le résultat. Pour le troisième point, l'injectivité est clair. Il faut montrer que l'on a bien un morphisme, cela vient du constat suivant :

$$(n,1)(n',1) = (nn',1)$$

Pour le quatrième point, on vérifie simplement que :

$$(1,k)(1,k') = ({}^k 1, kk') = (1,kk')$$

Le 5ème point est une conséquence du quatrième. Pour le 6ème, on constate que les 3 conditions du produit semi-direct interne sont réunis d'où le résultat. Le dernier point c'est le 1er calcul de la démo. ■

Proposition VII.5 Soit $G = N \rtimes_\alpha K$. Le produit est direct si et seulement si α est trivial.

Démonstration. Si le produit est direct alors K centralise N et par conséquent α est trivial via le dernier point de proposition précédente. La réciproque est triviale. ■

R Attention, on peut avoir $N \rtimes_\alpha K \simeq N \times K$ avec α non-trivial. Le contre-exemple classique est : pour tout $\alpha : \mathbb{Z}_{/2\mathbb{Z}} \to \mathrm{Aut}(\mathfrak{S}_3)$, on a $\mathfrak{S}_3 \rtimes_\alpha \mathbb{Z}_{/2\mathbb{Z}} \simeq \mathfrak{S}_3 \times \mathbb{Z}_{/2\mathbb{Z}}$.

4. Quelques groupes d'automorphismes

En général, le calcul de $\mathrm{Aut}(G)$ est quelque chose de difficile. Cependant, on peut retenir la proposition suivante :

Proposition VII.6 Soit p un nombre premier et $n \in \mathbb{N}$. On a :

$$\mathrm{Aut}_{\mathrm{gp}}((\mathbb{Z}/n\mathbb{Z},+)) = ((\mathbb{Z}/n\mathbb{Z})^\times,\times) \qquad \text{et} \qquad \mathrm{Aut}_{\mathrm{gp}}((\mathbb{Z}/p\mathbb{Z}^n,+)) = \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$$

Démo en exo. L'application $m : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}_{\mathrm{gp}}(\mathbb{Z}/n\mathbb{Z})$ définie par : $a \mapsto m_a$ où $m_a(x) = ax$ est un morphisme injectif de groupe. Montrons que m est surjective.

Soit α un automorphisme de $\mathbb{Z}/n\mathbb{Z}$. On pose $a := \alpha(1)$. On a donc :

$$\alpha(0) = m_a(0) \quad \text{et} \quad \alpha(1) = m_a(1)$$

Enfin,

$$\alpha(2) = \alpha(1+1) = \alpha(1) + \alpha(1) = a + a = 2a = m_a(2)$$

Par une récurrence immédiate, on obtient que $\alpha = m_a$.

On procède de façon similaire pour montrer que : $\mathrm{Aut}_{\mathrm{gp}}((\mathbb{Z}/p\mathbb{Z}^n,+)) = \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. On a un morphisme injectif $M : \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z}) \to \mathrm{Aut}_{\mathrm{gp}}((\mathbb{Z}/p\mathbb{Z}^n,+))$ définie par $A \mapsto M_A$ où $M_A(V) = AV$. Pour montrer que M est surjective, on procède comme précédemment.

Soit α un automorphisme. On note $A_i = \alpha(e_i)$ et on note $A = (A_1 \cdots A_n)$. Il reste à vérifier que $\alpha = M_A$. Soit V quelconque, on a $V = \sum \lambda_i e_i$. Le point crucial étant que les $\lambda_i \in \mathbb{Z}/p\mathbb{Z}$ donc sont représentés par $0, 1, ..., p-1$ des entiers.

Donc :

$$\alpha(V) = \alpha(\sum \lambda_i e_i) = \sum(\lambda_i e_i) = \sum \lambda_i \alpha(e_i) = \sum \lambda_i A_i = AV$$

■

R Le groupe $\mathrm{Aut}_{\mathrm{gp}}((\mathbb{Z}/n\mathbb{Z},+))$ est donc abélien (et fini). On peut chercher à calculer sa décomposition en produit de groupes cycliques. Voir le Perrin.

5. Isomorphisme entre deux produits semi-directs externes

Proposition VII.7 — A faire chez soi. Soient $\alpha_1, \alpha_2 : K \to \mathrm{Aut}(N)$. S'ils existent un φ :

$\mathrm{Aut}(K)$ et $\gamma \in \mathrm{Aut}(N)$ tel que :

$$\alpha_2(k) = \gamma \circ \alpha_1(\varphi(k)) \circ \gamma^{-1}$$

Alors, les produits semi-directs $N \rtimes_{\alpha_1} K$ et $N \rtimes_{\alpha_2} K$ sont isomorphes.

Proposition VII.8 — Application. Il existe une unique extension non-triviale de $(\mathbb{Z}/2\mathbb{Z})^2$ par $\mathbb{Z}/3\mathbb{Z}$.

Démonstration. Toute extension de $(\mathbb{Z}/2\mathbb{Z})^2$ par $\mathbb{Z}/3\mathbb{Z}$ est scindée donc donnée par un morphisme de $\mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})^2) = \mathrm{GL}_2(\mathbb{F}_2) \simeq {}^2\mathfrak{S}_3$. Le groupe $\mathfrak{S}_3$ possède deux éléments d'ordre 3, c'est deux éléments sont conjugués. A priori, il y a deux extensions possibles mais elles donnent des groupes isomorphes, via une post-conjugaison. ■

6. Produit semi-direct : point de vue suite exacte

Définition VII.5 Une *suite exacte* de groupes est la donnée de trois groupes N, G, K et deux morphismes $i : N \to G$ et $p : G \to K$ tel que :

1. i est injectif.
2. p est surjectif.
3. $\mathrm{Im} i = \ker p$.

On note :

$$1 \to N \xrightarrow{i} G \xrightarrow{p} K \to 1$$

R Soit G un groupe. Si N est un sous-groupe distingué de G et K est un groupe isomorphe à G/N alors on a une suite exacte :

$$1 \to N \to G \to K \to 1$$

avec i égale à l'inclusion, p égale à la projection sur G/N puis l'isomorphisme avec K. On dit que G est une *extension* de N par K.

Définition VII.6 Une suite exacte $1 \to N \to G \to K \to 1$ est *scindée* lorsqu'il existe un morphisme $s : K \to G$ tel que $p \circ s : K \to K = \mathrm{Id}$. Un tel morphisme s s'appelle une *section*.

R Une section est nécessairement injective.

R Une suite exacte $1 \to N \to G \to K \to 1$ est scindée si et seulement s'il existe un sous-groupe $\overline{K}$ de G tel que $p : \overline{K} \to K$ est un isomorphisme.

Proposition VII.9 Supposons que $G = N \rtimes K$ alors la suite exacte canonique $1 \to N \to G \to K \to 1$ (i.e. i égale à l'inclusion, $p(nk) = k$) est scindée par s l'inclusion $s : K \to G$.

Démonstration. On prend le point de vue externe. On a :

$$p \circ s(k) = p(1, k) = k.$$

■

2. Car de cardinal 6 et non abélien.

Proposition VII.10 Soit $1 \to N \to G \to K \to 1$ une suite exacte scindée par s. On définit une action α de K sur N par :

$$\alpha(k) \cdot h = s(k)\, h\, s(k)^{-1}$$

Le groupe G est égale au produit semi-direct interne de $i(N)$ par $s(K)$ et isomorphe au produit semi-direct externe de N par K relativement à α.

Démonstration. On vérifie les 3 points.

1. Le sous-groupe $i(N) = \ker(p)$ est bien distingué.
2. On a $i(N) \cap s(K) = \{1\}$:
   - En effet, soit $g \in i(N) \cap s(K)$.
   - $g \in i(N) = \ker(p)$ et $g = s(k)$ pour un certain $k \in K$.
   - $p(g) = p \circ s(k) = k = 1$.
   - Donc $k = 1$ et par suite $g = s(k) = 1$.
3. Enfin, $i(N)s(K) = G$ car :
   - Soit $g \in G$, on pose $k := p(g)$ et $n := gs(k)^{-1}$ (pas le choix !).
   - On doit vérifier que $n \in i(N) = \ker(p)$.
   - $p(n) = p(g)(p \circ s(k))^{-1} = kk^{-1} = 1$.

Le second point est une conséquence de la partie produit semi-direct externe. ■

Fin du cours 2

Définition VII.7 Une extension G de N par K donnée par une suite exacte $1 \to N \to G \to K \to 1$ est dite *triviale* lorsqu'elle est scindée et que $s(K)$ centralise $i(N)$. Autrement dit, lorsque $G = i(N) \times s(K)$.

Exercice 1.4 Reprendre les exemples de la partie produit semi-direct interne, écrire les suites exactes correspondantes, et trouver les sections s correspondantes. ∎

7. Extension centrale

Définition VII.8 Le groupe G est une *extension centrale* du groupe A par le groupe K lorsqu'il existe une suite exacte $1 \to A \to G \to K \to 1$ tel que $i(A)$ est inclus dans le centre de G.

- Pour tout groupe, on a :
$$1 \to Z \to G \to G/Z \to 1$$
Donc tout groupe à centre non-trivial est une extension centrale.
- Ceci sera utile pour les deux groupes $\mathrm{GL}_n(k)$ et $\mathrm{SL}_n(k)$.
  - ◇ Le groupe $\mathrm{GL}_n(k)$ est une extension centrale du groupe $Z(\mathrm{GL}_n(k)) \simeq k^*$ par le groupe $\mathrm{PGL}_n(k)$.
  - ◇ Le groupe $\mathrm{SL}_n(k)$ est une extension centrale du groupe $Z(\mathrm{SL}_n(k)) \simeq \mu_n(k) = \{\lambda \in k \mid \lambda^n = 1\}$ par le groupe $\mathrm{PSL}_n(k)$.
- Les extensions centrales ça existent.. .
- **Une extension centrale et scindée est triviale, i.e** $G = A \times K$**,** puisque K centralise A, puisque A est dans le centre ... Donc une extension centrale non-triviale n'est pas un produit semi-direct.
- Les deux exemples de cette liste ne sont pas des produits directs sauf dans des cas particuliers (par exemple : $k = \mathbb{F}_2$ pour le premier, et $\mu_n(k) = 1$ pour le second.) Voir un TD futur pour un énoncé précis des exceptions.
- Bref, ce qu'il faut retenir c'est qu'ils existent des extensions qui ne sont pas des produits semi-directs (même dans des cadres très naturels).
- Attention à $\mathrm{GL}_n(k)$. Il y a deux suites exactes naturelles pour $\mathrm{GL}_n(k)$:
  - ◇ $1 \to \mathrm{SL}_n(k) \to \mathrm{GL}_n(k) \xrightarrow{\text{dét}} k^\times \to 1$, extension scindée qui donne un produit semi-direct.
  - ◇ $1 \to Z(\mathrm{GL}_n(k)) \to \mathrm{GL}_n(k) \to \mathrm{PGL}_n(k) \to 1$, extension centrale non-triviale, non scindée (en général). $Z(\mathrm{GL}_n(k)) \simeq k^\times$

VIII Les groupes diédraux

Définition VIII.1 Le *groupe diédral d'ordre* $2n$ est le produit semi-direct du groupe $\mathbb{Z}/n\mathbb{Z}$ par le groupe $\mathbb{Z}/2\mathbb{Z}$ via l'automorphisme $\alpha(1) \cdot x = -x$. Le *groupe diédral d'ordre infini* est le produit semi-direct du groupe $\mathbb{Z}$ par le groupe $\mathbb{Z}/2\mathbb{Z}$ via l'automorphisme $\alpha(1) \cdot x = -x$. On le note[a] $\mathbb{D}_n$ (resp. $\mathbb{D}_\infty$).

a. La notation $\mathbb{D}_{2n}$ est aussi très répandu, ce qui crée une confusion constante et uniforme...

Proposition VIII.1 Un groupe G est isomorphe au groupe diédral d'ordre $2n$ (resp. infini) si et seulement s'il est engendré par deux éléments a et b tels que a est d'ordre n (resp. infini), b est d'ordre 2 et $bab^{-1} = a^{-1}$.

Proposition VIII.2 Soit G un groupe. Si G est engendré par deux éléments d'ordre deux (distincts) alors G est un groupe diédral.

Démonstration. On note b et c les deux éléments d'ordre 2. On note $a = bc$. On a :

$$\langle b,c\rangle = \langle a,b\rangle \quad bab^{-1} = b(bc)b = cb = a^{-1}$$

■

Proposition VIII.3 Pour $n \geqslant 3$, le groupe des isométries du polygone régulier à n côtés est le groupe diédral d'ordre $2n$.

Démonstration. Pour se simplifier la vie, on prend pour polygone régulier $\mathcal{P}_n$ à n côtés, l'enveloppe convexe des racines n-ièmes de l'unité. Ainsi, le groupe G engendré par la rotation d'angle $2\pi/n$ et la conjugaison complexe est inclus dans S le groupe de symétrie de $\mathcal{P}_n$.

Soit $g \in S$, comme l'action de G sur les sommets de $\mathcal{P}_n$ est transitive, on peut supposer que g fixe le sommet $1 \in \mathbb{C}$ de $\mathcal{P}_n$. Or une isométrie qui fixe 0 et 1 est l'identité ou la conjugaison complexe. Donc $g \in G$, par suite $G = S$. ■

R Dans ce cas, le groupe diédral est engendré par les matrices suivantes :

$$a = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \qquad b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Exercice 1.5 Montrer que :

- Le centre de $\mathbb{D}_n$ est trivial si n est impair ou infini.
- Si n est pair alors son centre est le sous-groupe d'ordre 2, $\{1, a^{n/2}\}$.
- Le groupe dérivé de $\mathbb{D}_n$ est le groupe $\langle a\rangle$ si n est impair.
- Si n est pair ou infini alors son groupe dérivé est le sous-groupe $\langle a^2\rangle$.
- Si n est impair[a] ou infini alors toutes les réflexions sont conjugées.
- Sinon, il y a deux classes de conjugaison.

■

a. Conséquence du théorème de Sylow.

IX Les groupes symétriques et les groupes alternés

1. Le vocabulaire de base

Le groupe symétrique d'un ensemble fini X est le groupe des bijections de X, on le note $\mathfrak{S}(X)$. Lorsque $X = \{1,\dots,n\}$, on le note $\mathfrak{S}_n$.

Proposition IX.1 Le groupe $\mathfrak{S}_n$ est engendré par les transpositions.

Corollaire IX.2 — Définition du groupe alterné $\mathfrak{A}_n$.

- Soit σ une permutation. Si σ est le produit de k transpositions alors on note $\varepsilon(\sigma) := (-1)^k$.

- L'application $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est bien définie et est un morphisme de groupes.
- Le noyau de ce morphisme s'appelle le *groupe alterné*, on le note $\mathfrak{A}_n$.

2. Transitivité multiple

Proposition IX.3 L'action de $\mathfrak{S}_n$ sur $\{1,\dots,n\}$ est simplement n-transitive. L'action de $\mathfrak{A}_n$ sur $\{1,\dots,n\}$ est simplement $(n-2)$-transitive.

Démonstration. Le cas de l'action de $\mathfrak{S}_n$ sur $\{1,\dots,n\}$ est trivial. On ne fait que le cas de $\mathfrak{A}_n$. Soient $x_1,\dots,x_{n-2}$ et $y_1,\dots,y_{n-2}$. Il existe une permutation $\sigma \in \mathfrak{S}_n$ tel que $\sigma(x_i) = y_i$. Si $\sigma \in \mathfrak{A}_n$ alors c'est fini. Sinon, soient x_{n-1}, x_n les deux éléments manquants. On note $y_{n-1} = \sigma(x_{n-1})$ et $y_n = \sigma(x_n)$. Alors, $(y_{n-1}\, y_n)\sigma \in \mathfrak{A}_n$ et vérifie le cahier des charges.

Reste à montrer que l'action est simplement $(n-2)$-transitive. Il faut montrer que le stabilisateur de $n-2$ points distincts est trivial. Le stabilisateur de $n-2$ points distincts dans $\mathfrak{S}_n$ est engendré par la transposition qui échange les deux points restants, ce n'est pas une permutation paire. ■

3. Les 3-cycles dans $\mathfrak{A}_n$

Proposition IX.4 Si $n \geqslant 5$ alors deux 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Démonstration. Principe de conjugaison :

$$g(i_1\, i_2 \cdots i_k)g^{-1} = (g(i_1)\, g(i_2) \cdots g(i_k))$$

Si $n \geqslant 5$ alors l'action de $\mathfrak{A}_n$ est 3-transitive. Ensuite, on applique le principe de conjugaison. ■

Proposition IX.5 Si $n \geqslant 3$ alors le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles.

Démonstration. Toute permutation paire est le produit d'un nombre paire de transpositions. Il suffit donc de montrer que (sans perte de généralités) :

$$(12)(34) \qquad \text{et} \qquad (12)(13)$$

sont des produits de 3-cycles. Or, on a :

$$(12)(34) = (314)(123) \qquad \text{et} \qquad (12)(13) = (132)$$

■

4. Centres

Proposition IX.6 Le centre de $\mathfrak{S}_n$ (resp. $\mathfrak{A}_n$) est trivial pour $n \geqslant 3$ (resp. $n \geqslant 4$).

R Les groupes $\mathfrak{S}_1$, $\mathfrak{S}_2$, $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{A}_3$ sont abéliens d'ordres respectifs : $1, 2, 1, 1, 3$.

Démonstration. Soit $\sigma \in \mathfrak{S}_n$ non-trivial et central. Quitte à renuméroter, on peut supposer que $\sigma(1) = 2$. Calculons alors $\sigma(13)\sigma^{-1} = (\sigma(1)\sigma(3)) = (2\sigma(3)) \neq (13)$. Absurde.

Soit $\sigma \in \mathfrak{A}_n$ non trivial et central. Quitte à renuméroter, on peut supposer que $\sigma(1) = 2$. Calculons alors $\sigma(134)\sigma^{-1} = (\sigma(1)\sigma(3)\sigma(4)) = (2\sigma(3)\sigma(4)) \neq (134)$. Absurde. ■

5. Groupes dérivés

Proposition IX.7 Le groupe dérivé de $\mathfrak{S}_n$ (resp. $\mathfrak{A}_n$) est $\mathfrak{A}_n$ pour $n \geqslant 1$ (resp. $n \geqslant 5$).

Démonstration. La première affirmation est triviale pour $n = 1,2$. Pour $n \geqslant 3$, l'égalité $[(12),(13)] = (12)(13)(12)(13) = (231)$ montre que le groupe dérivé contient un 3-cycle, il les contient donc tous puisqu'il est distingué. Mais les 3-cycles engendrent $\mathfrak{A}_n$. Donc $\mathfrak{A}_n \leqslant \mathfrak{S}_n'$. L'autre inclusion est triviale puisque tout commutateur est une permutation paire.

La seconde est triviale si on utilise la simplicité de $\mathfrak{A}_n$, le groupe dérivé étant non-trivial puisque $\mathfrak{A}_n$ n'est pas commutatif pour $n \geqslant 5$. On se refuse à utiliser un marteau pour tuer une mouche. On peut simplement remarquer que $[(123),(145)] = (123)(145)(132)(154) = (142)$. Par conséquent, pour $n \geqslant 5$, le groupe dérivé contient un 3-cycle. On conclut comme précdemment. ■

R Le groupe dérivé de $\mathfrak{A}_n$, pour $n = 1,2,3$ sont triviaux puisque $\mathfrak{A}_n$ est abélien. Le groupe dérivé de $\mathfrak{A}_4$ est le groupe des doubles transpositions souvent noté $V_4 \simeq \mathbb{Z}/2\mathbb{Z}^2$.

6. Simplicité

Théorème IX.8 Le groupe $\mathfrak{A}_n$ est simple, pour $n \geqslant 5$.

Exercice 1.6 On note $\mathfrak{S}_\infty$ le groupe des bijections de $\mathbb{N}$ à support fini. On note $\mathfrak{A}_\infty$ le noyau du morphisme signature[a]. Montrer que $\mathfrak{A}_\infty$ est simple. ■

a. Vérifier qu'il est bien défini !

Proposition IX.9 Les sous-groupes distingués de $\mathfrak{S}_n$ pour $n \geqslant 5$ sont $1, \mathfrak{A}_n$ et $\mathfrak{S}_n$.

R Les sous-groupes distingués de $\mathfrak{S}_4$ sont $1, V_4, \mathfrak{A}_4$ et $\mathfrak{S}_4$.

R Les sous-groupes distingués de $\mathfrak{S}_3$ sont $1, \mathfrak{A}_3$ et $\mathfrak{S}_3$.

X Groupes résolubles

1. C'est quoi ?

Définition X.1 Soit G un groupe G. Une *suite de composition* est une suite finie de sous-groupes

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_{n-1} \geqslant G_n = \{e\}$$

tel que, pour tout $i = 0, \ldots, n-1$, G_{i+1} est distingué dans G_i. Les quotients G_i/G_{i+1} s'appelle les *quotients/facteurs* de la suite de composition. Une suite de composition est dite de *Jordan-Hölder* lorsque tous ses facteurs sont simples non-triviaux.

Théorème X.1 — Théorème de Jordan-Hölder. Tout groupe fini admet une suite de Jordan-Hölder. Les facteurs d'une suite de Jordan-Hölder sont unique à permutation près.

R On ne demande pas aux groupes G_i d'être distingués dans G, seulement d'être distingués dans G_{i-1}.

Définition X.2 Un groupe G est dit *résoluble* lorsqu'il admet une suite de composition dont les quotients sont abéliens.

Proposition X.2 Un groupe G est résoluble si et seulement s'il existe un entier k tel que $D^{(k)}(G) = \{e\}$.

Démonstration. Supposons qu'il existe un entier k tel que $D^{(k)}(G) = \{e\}$. Alors on prend $G_i = D^{(i)}(G)$, les conditions sont vérifées, par définition du groupe dérivé.

Supposons G résoluble. Il existe une suite finie :

$$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_{n-1} \geqslant G_n = \{e\}$$

tel que, pour tout $i = 0, \ldots, n-1$:

- G_{i+1} est distingué dans G_i.
- Le quotient G_i/G_{i+1} est abélien.

En particulier, G_0/G_1 est abélien donc $D(G) \leqslant G_1$. De même, G_1/G_2 est abélien donc $D(G_1) \leqslant G_2$, mais $D^{(2)}(G) \leqslant D(G_1) \leqslant G_2$. Par récurrence, on obtient $D^{(i)}(G) \leqslant G_i$, pour tout i. Ainsi, pour $k = n$, on obtient le résultat. ■

On laisse la proposition suivante en exercice.

Proposition X.3 Un groupe **fini** G est *résoluble* si et seulement s'il admet une suite de composition dont les facteurs sont cycliques d'ordre premier.

2. Propriétés

Proposition X.4 Être résoluble est une propriété très stable. Plus précisément,

- Tout sous-groupe et tout quotient d'un groupe résoluble est résoluble.
- Supposons $N \lhd G$. Alors G est résoluble si et seulement si N et G/N sont résolubles.
- Un groupe simple est résoluble si et seulement s'il est cyclique d'ordre premier.

Fin du cours 3

On aura besoin du lemme suivant.

Lemma X.5 Soit $K \lhd L \leqslant G$. Pour tout morphisme $f : G \to H$, on a $f(K) \lhd f(L)$ et $f : L \to f(L)$ induit un morphisme surjectif $f : L/K \to f(L)/f(K)$.

Démonstration. Le premier point est une vérification élémentaire. Soient $y \in f(L)$, $v \in f(K)$... Pour le second point, le morphisme surjectif $f : L \to f(L)$ induit un morphisme surjectif $f : L \to f(L)/f(K)$ de noyau contenant K, d'où le morphisme induit. ■

Démonstration. La première assertion est claire si on se rappelle que $D(G) \subset D(H)$ dès que $G \subset H$. Pour la seconde assertion, on peut la reformuler de la façon suivante, soit $f : G \to H$ un morphisme surjectif. Si G est résoluble alors H est résoluble. En effet, si

$$\{e\} = G_n \leqslant G_{n-1} \leqslant G_{n-2} \leqslant \cdots \leqslant G_1 \leqslant G_0 = G$$

est une suite de composition dont les facteurs sont abéliens alors :

$$\{e\} = f(G_n) \leqslant f(G_{n-1}) \leqslant f(G_{n-2}) \leqslant \cdots \leqslant f(G_1) \leqslant f(G_0) = f(G) = H$$

est une suite de composition, puisque l'image d'un groupe distingué par un morphisme surjectif est un groupe distingué, par le lemme précédent. Enfin, le morphisme $f : G_i \to f(G_i)$ induit un morphisme surjectif $G_i/G_{i+1} \to f(G_i)/f(G_{i+1})$, donc $f(G_i)/f(G_{i+1})$ est un groupe abélien, puisque G_i/G_{i+1} est abélien.

Il faut à présent montrer que N et G/N résolubles entraine G résoluble. On se donne une suite de composition dont les facteurs sont abéliens pour N et G/N :

$$\{e\} = N_n \leqslant N_{n-1} \leqslant N_{n-2} \leqslant \cdots \leqslant N_1 \leqslant N_0 = N$$

$$\{e\} = K_m \leqslant K_{m-1} \leqslant K_{m-2} \leqslant \cdots \leqslant K_1 \leqslant K_0 = G/N$$

On relève [3] la seconde en une suite de composition qui va de N à G :

$$N = L_m \leqslant L_{m-1} \leqslant L_{m-2} \leqslant \cdots \leqslant L_1 \leqslant L_0 = G$$

Le tout forme une suite de composition pour G. En effet, la condition de distinction est évidente. La condition de quotient abélien est évidente pour le bout de $\{e\}$ à N et pour le bout de N à G, cela est dû au fait que $L_i/L_{i-1} \simeq \frac{L_i/N}{L_{i-1}/N} \simeq K_i/K_{i-1}$.

Soit G groupe résoluble simple. On considère une suite de composition de G dont les facteurs sont abéliens non-triviaux. Le groupe G étant simple, il ne peut avoir de groupe distingué, donc la suite de composition considérée est réduite à deux éléments. Donc G est abélien. Dans un groupe abélien, tout groupe est distingué. Donc G ne peut avoir de sous-groupes propres puisqu'il est simple. Le Théorème de Cauchy affirme que pour tout diviseur premier p de l'ordre de G, G possède un groupe d'ordre p. Par conséquent, G doit être cyclique d'ordre premier. On vérifie sans peine qu'un tel groupe est simple par le théorème de Lagrange. ■

3. Rappel : Le morphisme $G \to G/N$ induit une bijection entre les sous-groupes de G/N et les sous-groupes de G contenant N. Cette bijection respecte la normalité. Enfin, si $N \leqslant K \lhd G$ alors $\frac{G/N}{K/N} \simeq G/K$ via l'application naturelle (3^{eme} théorème d'isomorphisme).

3. Exemples

R Les groupes abéliens sont résolubles. Les extensions de groupes abéliens. En particulier les produits directs et semi-directs de groupes abéliens par un groupe abélien sont résolubles.

Proposition X.6 — L'exemple n°1 à retenir. Le groupe des matrices triangulaires supérieures et ses sous-groupes (sur un corps quelconque) sont résolubles.

Démonstration. On note :

$$\mathrm{T}_n(k) = \begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix} \qquad \mathrm{U}_n(k) = \begin{pmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathrm{U}_n^{-1}(k) = \begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & 0 & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \mathrm{U}_n^{-2}(k) = \begin{pmatrix} 1 & 0 & 0 & * \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Ou de façon plus formel :

- $\mathrm{T}_n(k) = \{M \in \mathrm{GL}_n(k) \,|\, M_{i,j} = 0,\ \forall i > j\}$
- $\mathrm{U}_n(k) = \{M \in \mathrm{T}_n(k) \,|\, M_{i,i} = 1,\ \forall i\}$
- $\mathrm{U}_n^{-1}(k) = \{M \in \mathrm{U}_n(k) \,|\, M_{i,j} = 0,\ \forall i - j = -1\}$
- $\mathrm{U}_n^{-l}(k) = \{M \in \mathrm{U}_n(k) \,|\, M_{i,j} = 0,\ \forall i - j = -1, \ldots, -l\}$

On fait ensuite les calculs suivants, dont on conseille de retenir le résultat. On a :

- $[T_n, T_n] \leqslant U_n$
- $[U_n, U_n] \leqslant U_n^{-1}$
- $[U_n^{-k}, U_n^{-k}] \leqslant U_n^{-k-1}$
- $D^{(n)}(T_n) = 1$

La première affirmation est conséquence du fait que si $g \in T_n$ alors :

$$(g^{-1})_{ii} = (g_{ii})^{-1}$$

La seconde affirmation vient du fait si $g \in U_n$ alors :

$$(g^{-1})_{i,i+1} = -g_{i,i+1}$$

La troisième affirmation vient du fait si $g \in U_n^{-l}$ alors :

$$(g^{-1})_{i,i+l-1} = -g_{i,i+l-1}$$

■

Définition X.3 Soit p un nombre premier. Un p-groupe est un groupe fini d'ordre une puissance de p.

Proposition X.7 Le centre d'un p-groupe est non-trivial.

Proposition X.8 — L'exemple n°2 à retenir. Tout $p-$groupe est résoluble.

Démonstration. Simple application du fait que le centre d'un p-groupe est non-trivial via une récurrence forte sur l'ordre du p-groupe. ■

Exercice 1.7 Tout groupe d'ordre < 60 est résoluble. Stratégie :

- On vient de voir que les groupes d'ordre p^α sont résolubles.
- Montrer en utilisant les théorèmes de Sylow que tout groupe d'ordre $n = pq^\alpha$ ou $n = p^2q$ avec $p < q$ est résoluble, attention le cas $n = 12$ doit être fait à part.
- Les entiers de 1 à 59 qui ne sont pas de la forme $n = pq^\alpha$, p^α, et p^2q sont :

$$24, 30, 36, 40, 42, 48, 56$$

  Ils sont donc ou bien de la forme :

$$pqr \quad \text{comme} \quad 30, 42$$

  ou de la forme :

$$2^\alpha p \quad \text{comme} \quad 24, 40, 48, 56$$

  ou le rebel de la famille :

$$36 = 2^2 \cdot 3^2$$

- Un argument de comptage montre que les groupes de cardinal pqr doivent avoir l'un de leurs Sylow distingués.
- Les groupes d'ordre $2^\alpha \cdot 3$ avec $\alpha \geqslant 2$ qui vérifie $s_2 = 3$ possède un morphisme non-trivial $\varphi : G \to \mathfrak{S}_3$, de noyau non-trivial...
- On peut vérifier à la main que pour $n = 40, 56$, $s_{big} = 1$ parce que tous les diviseurs de m ne sont pas congrus à 1 modulo big...
- Reste 36... On applique l'argument d'action sur les 3-Sylows, i.e. $36 \nmid 2^2$!

■

Théorème X.9 Deux théorèmes célèbres et difficiles :

- Théorème de Burnside (1904) : tout groupe d'ordre $p^a q^b$ est résoluble.
- Théorème de Feit-Thompson (1963) : tout groupe d'ordre impair est résoluble.

4. Non-exemples

- Les groupes $\mathfrak{S}_n$ et $\mathfrak{A}_n$ ne sont pas résolubles ssi $n \geqslant 5$.
- Les groupes $\mathrm{GL}_n(k)$, $\mathrm{SL}_n(k)$, $\mathrm{PSL}_n(k)$, $\mathrm{PGL}_n(k)$ et $\mathrm{GA}_n(k)$ ne sont résolubles que si $n = 1$ et k quelconque ou $(n, k) = (2, \mathbb{F}_2)$ ou $(2, \mathbb{F}_3)$.
- Le groupe libre (pour ceux qui le connaissent) n'est pas résoluble.

5. Pourquoi le mot résoluble ?

A tout polynôme P à coefficient dans $\mathbb{Q}$, on peut associer un corps K_P qui est $\mathbb{Q}$ plus toutes les racines de P (corps de décomposition de P), peut-être croiser en THNO...

Depuis la nuit des temps, on se demande s'ils existent des formules qui permettent de calculer les racines de P à l'aide des coefficients de P, formule qui ne feraient intervenir que les coefficients et les opérations : $+,-,\times,/$ et les racines n-ièmes.

On apprend au lycée à calculer les racines d'un polynôme de degré 2, on apprend parfois à l'université à trouver les racines d'un polynôme de degré 3 (Tartaglia, ~ 1535). En fait, il y aussi des formules pour le degré 4 (bon exo de L3-M1, voir le livre de JP Escoffier), trouvées par Ferrari, ~ 1555.

Après, ça coince... Abel en 1824 et Galois en 1830 montre qu'il n'y a pas de formules... C'est quoi l'idée ?

Galois étant donné un corps K contenant $\mathbb{Q}$, Galois introduit le groupe de Galois :

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma \in \mathrm{Aut}(K) \,|\, \sigma_{|\mathbb{Q}} = \mathrm{Id}\}$$

Galois montre que les racines de P s'expriment par radicaux si et seulement si le groupe $\mathrm{Gal}(K_P/\mathbb{Q})$ est résoluble. Il montre aussi que $\mathrm{Gal}(K_P/\mathbb{Q}) \simeq \mathfrak{S}_5$ si $x^5 - 4x + 2$ [4].

XI Groupes nilpotents

1. Vocabulaire préliminaire

2. C'est quoi ?

Définition XI.1 Soit G un groupe. La *suite centrale descendante* de G, notée $(C_i(G))_{i\geqslant 1}$ est définie par récurrence :

- $C_0(G) = G$
- $C_{i+1}(G) = [C_i(G), G]$

R On a toujours $C_1(G) = [G,G] = D(G)$

Définition XI.2 Un groupe est dit *nilpotent* lorsqu'il existe un entier n tel que $C_n(G) = 1$.

Proposition XI.1 Les groupes résolubles sont nilpotents.

R [A retenir]

$$\text{Abélien} \subset \text{Nilpotent} \subset \text{Résoluble}$$

Démonstration. Par définition, on a :

$$D^{(i)}(G) \leqslant C_i(G)$$

Or résoluble signifie qu'il existe un n tel que $D^{(n)}(G) = 1$. ∎

R Le groupe $\mathfrak{S}_3$ n'est pas nilpotent (bien qu'il soit résoluble).

- $C_1(\mathfrak{S}_3) = \mathfrak{A}_3$
- $C_2(\mathfrak{S}_3) = [\mathfrak{A}_3, \mathfrak{S}_3] = \mathfrak{A}_3$ puisque $[(12),(123)] = (123)$.
- et donc $C_n(\mathfrak{S}_3) = \mathfrak{A}_3$, $\forall n \geqslant 1$.

4. Ca marche pour tout polynôme irréductible de degré 5 possédant exactement 3 racines réelles.

3. Propriétés évidentes

Proposition XI.2 Les sous-groupes et les quotients de groupes nilpotents sont nilpotents. Les produits directs de groupes nilpotents sont nilpotents.

R Attention : les produits semi-directs de groupes nilpotents n'ont aucune raison d'être nilpotents, ils sont néanmoins résolubles...

Démonstration. Pour les sous-groupes : tout simplement car si $H \leqslant G$ alors pour tout i, $C_i(H) \leqslant C_i(G)$. Pour les quotients : Soit G un groupe nilpotent et $f : G \to L$ un morphisme surjectif. On doit montrer que L est nilpotent. On a, par récurrence cachée :

$$C_i(L) = [C_{i-1}(L), L] = [f(C_{i-1}(G)), f(G)] \leqslant f([C_{i-1}(G), G]) = f(C_i(G))$$

Pour les produits directs. Tout simplement parce que $C_i(H \times K) \leqslant C_i(H) \times C_i(K)$. ■

4. Premier exemple

Proposition XI.3 Le groupe de matrices triangulaires supérieures avec des 1 sur la diagonale de taille n sur un corps k, noté $\mathrm{U}_n(k)$ est nilpotent.

Démonstration. On calcul que $[U_n, U_n] \leqslant U_n^{-1}$, et puis que $[U_n^{-1}, U_n] \leqslant U_n^{-2}$ ■

R Le groupe $T_n(k)$ n'est pas nilpotent si $n \leqslant 2$.

5. La suite centrale ascendante

Définition XI.3 Soit G un groupe la suite centrale ascendante est la suite de sous-groupes $Z_i(G)$ définie par :

1. $Z_0(G) = 1$
2. $Z^{i+1}(G)$ est l'image inverse du centre de $G/Z^i(G)$ via la projection canonique $\nu_i : G \to G/Z^i(G)$.
3. $Z^{i+1}(G)/Z^i(G) = Z(G/Z^i(G))$

R Par une récurrence immédiate, les sous-groupes $Z^i(G)$ sont des sous-groupes caractéristiques de G.

R On a $Z_0(G) = 1$, donc $Z_1(G)$ est l'image réciproque du centre de $G/1$ via $G \to G/1$, autrement dit $Z_1(G) = Z(G)$.
Ensuite, $Z_2(G)$ est l'image réciproque du centre de G/Z via l'application $G \to G/Z$

Lemma XI.4 Soit G un groupe et deux sous-groupes H, K tels que $K \lhd G$ et $K \leqslant H \leqslant G$. Alors :

$$[H, G] \leqslant K \quad \Leftrightarrow \quad H/K \leqslant Z(G/K).$$

Démonstration. Soient $g \in G, h \in H$, on a :

$$hKgK = gKhK \Leftrightarrow hgK = ghK \Leftrightarrow [h, g]K = K \Leftrightarrow [h, g] \in K$$

■

Proposition XI.5 Soit G un groupe. Il existe un entier n tel que $Z^n(G) = G$ si et seulement si $C_n(G) = 1$. De plus dans ce cas, on a :

$$C_i \leqslant Z^{n-i}, \quad \forall i$$

En particulier, G est nilpotent si et seulement s'il existe un entier n tel que $Z^n(G) = G$.

Démonstration. Supposons que $Z^n = G$. Montrons par récurrence que :

$$C_i \leqslant Z^{n-i}, \quad \forall i$$

Pour $i = 0$, c'est trivial. Supposons que l'inégalité est vrai au rang i. On a alors :

$$C_{i+1} = [C_i, G] \leqslant [Z^{n-i}, G] \leqslant Z^{n-i-1}$$

Supposons que $C_n = 1$. Montrons par récurrence que :

$$C_{n-i} \leqslant Z^i, \quad \forall i$$

Pour $i = 0$, l'inclusion est évidente. Supposons qu'elle est vraie au rang i. L'inclusion $C_{n-i} \leqslant Z^i$ entraîne que le morphisme $G/C_{n-i} \to G/Z^i$ est surjectif. Par définition, on a :

$$[C_{n-i-1}, G] = C_{n-i} \quad \text{donc} \quad C_{n-i-1}/C_{n-i} \leqslant Z(G/C_{n-i})$$

Or (exo), si $f : G \to H$ est surjectif alors $f(Z(G)) \leqslant Z(H)$. On obtient donc :

$$C_{n-i-1}Z^i/Z^i \leqslant Z(G/Z^j) = Z^{i+1}/Z^i$$

Ainsi :

$$C_{n-i-1} \leqslant C_{n-i-1}Z^i/Z^i \leqslant Z^{i+1}.$$

■

Proposition XI.6 Le centre d'un groupe nilpotent est non-trivial.

Démonstration. En effet, si n est le plus petit entier tel que $C_n(G) = G$ alors $1 \neq C_{n-1}(G) \leqslant Z^1(G) = Z(G)$. ■

6. Deuxième exemple

Proposition XI.7 Les p-groupes finis sont nilpotents.

Démonstration. Rappel : Le centre d'un p-groupe est non-trivial. Montrons que la suite centrale ascendante est strictement croissante (jusqu'à G). Soit i tel que $Z^i < G$, montrons que $Z^{i+1} > Z^i$.

En effet, comme G/Z^i est un p-groupe, son centre est non-trivial, par conséquent, $Z^{i+1} > Z^i$. ■

7. Une remarque sur les produits de Sylow sans hypothèse sur G

Proposition XI.8 Soit G un groupe. On note p_1, ..., p_k k nombres premiers distincts qui divise l'ordre de G. On suppose que pour tout i, le p_i-Sylow P_i est distingué. Alors $H = P_1 \cdots P_k$ est un sous-groupe normal de G qui est le produit direct (interne) des P_i.

Démonstration. Si $k = 1$, c'est trivial. On fait le cas $k = 2$, le cas général est une récurrence aussi trivial que le cas $k = 2$. Le produit $H = P_1P_2$ est un sous-groupe de G puisque P_1 est distingué. Le sous-groupe H est distingué car P_1 et P_2 sont distingués, en effet soit $g, k_1, k_2 \in g \times P_1 \times P_2$ alors $gk_1k_2g^{-1}$ est bien dans P_1P_2.

Enfin, on a $P_1 \cap P_2 = 1$ puisque leurs ordres sont premiers entre eux. Il nous reste à montrer que $[P_1, P_2] = 1$ mais $[P_1, P_2] \leqslant [P_1, G] \leqslant P_1$ puisque P_1 est distingué. On a aussi $[P_2, G] \leqslant P_2$, d'où le résultat. ■

8. Un lemme sur les normalisateurs de Sylow sans hypothèse sur G

Proposition XI.9 Soit G un groupe fini. Soit P un p-Sylow alors $N_G(N_G(P)) = N_G(P)$.

Démonstration. Soit $g \in G$ qui normalise $N_G(P)$. On veut montrer que $g \in N_G(P)$, autrement dit que $gPg^{-1} = P$.

Le groupe gPg^{-1} est un sous-groupe de $N_G(P)$, c'est donc un p-Sylow de $N_G(P)$ puisque c'est un p-Sylow de G. Mais P est distingué dans $N_G(P)$ donc $N_G(P)$ ne possède qu'un seul p-Sylow : P donc $gPg^{-1} = P$. ■

9. Lemme du normalisateur spécifique au groupe nilpotent

Proposition XI.10 — Les sous-groupes des groupes nilpotents ne sont pas auto-normalisants. Soit G un groupe nilpotent et $H < G$ alors $H < N_G(H)$.

Démonstration. On rappelle la définition de $N_G(H)$... Puisque G est nilpotent, il existe un i tel que :

$$C_{i+1} \leqslant H \quad C_i \nleqslant G$$

On a :

$$[C_i, H] \leqslant [C_i, G] = C_{i+1} \leqslant H$$

donc C_i normalise H, donc $C_i \leqslant N_G(H)$ donc $H < N_G(H)$. ■

10. Description des groupes nilpotents via leurs Sylows

Théorème XI.11 Soit G un groupe fini. Les assertions suivantes sont équivalentes :

- Le groupe G est nilpotent.
- Tous les Sylows de G sont distingués.
- Le groupe G est le produit direct de ses Sylows.
- Tous les Sylows de G sont uniques.

Démonstration. L'implication $1 \Rightarrow 2$ est difficile et l'implication $2 \Rightarrow 3$ est non-évidente, le lemme sur les produits de Sylow fait le travail.

On montre à présent $1 \Rightarrow 2$, soit P un Sylow alors $N_G(P)$ est autonormalisant mais ceci n'est pas autorisé dans les groupes nilpotents sauf si $N_G(P) = G$ donc $N_G(P) = G$, ce qui sgnifie que P est distingué dans G. ■

A recaser, ou pas ...

R Si S est un sous-groupe de G alors l'action par translation de G sur G induit une action de G sur l'ensemble quotient G/S des classes à gauche de G modulo S, via $g \cdot xS := gxS$. Tout sous-groupe H de G agit donc (par translation à gauche) sur l'ensemble quotient G/S. Le stabilisateur pour cette action du point xS est le sous-groupe $H \cap xSx^{-1}$. Ainsi, si H fixe le point xS alors $H \subset xSx^{-1}$.

Order	Factor	nb gps/iso	nb non-ab/iso	list gps of given order up to iso.
1	1	1	0	
2	2	1	0	
3	3	1	0	
4	2^2	2	0	
5	5	1	0	
6	$2\cdot 3$	2	1	
7	7	1	0	
8	2^3	5	2	
9	3^2	2	0	
10	$2\cdot 5$	2	1	
11	11	1	0	
12	$2^2\cdot 3$	5	3	
13	13	1	0	
14	$2\cdot 7$	2	1	
15	$3\cdot 5$	1	0	
16	2^4	14	9	
17	17	1	0	
18	$2\cdot 3^2$	5	3	
19	19	1	0	
20	$2^2\cdot 5$	5	3	
21	$3\cdot 7$	2	1	
22	$2\cdot 11$	2	1	
23	23	1	0	
24	$2^3\cdot 3$	15	12	
25	5^2	2	0	
26	$2\cdot 13$	2	1	
27	3^3	5	2	
28	$2^2\cdot 7$	4	2	
29	29	1	0	
30	$2\cdot 3\cdot 5$	4	3	
31	31	1	0	
32	2^5	51	44	
33	$3\cdot 11$	1	0	
34	$2\cdot 17$	2	1	
35	$5\cdot 7$	1	0	
36	$2^2\cdot 3^2$	14	10	
37	37	1	0	
38	$2\cdot 19$	2	1	
39	$3\cdot 13$	2	1	
40	$2^3\cdot 5$	14	11	
41	41	1	0	
42	$2\cdot 3\cdot 7$	6	5	
43	43	1	0	
44	$2^2\cdot 11$	4	2	
45	$3^2\cdot 5$	2	0	
46	$2\cdot 23$	2	1	
47	47	1	0	

Order	Factor	nb gps/iso	nb non-ab/iso	list gps of given order up to iso.
48	$2^4 \cdot 3$	52	47	
49	7^2	2	0	
50	$2 \cdot 5^2$	5	3	
51	$3 \cdot 17$	1	0	
52	$2^2 \cdot 13$	5	3	
53	53	1	0	
54	$2 \cdot 3^3$	15	12	
55	$5 \cdot 11$	2	1	
56	$2^3 \cdot 7$	13	10	
57	$3 \cdot 19$	2	1	
58	$2 \cdot 29$	2	1	
59	59	1	0	
60	$2^2 \cdot 3 \cdot 5$	13	11	
61	61	1	0	
62	$2 \cdot 31$	2	1	
63	$3^2 \cdot 7$	4	2	
64	2^6	267	256	
65	$5 \cdot 13$	1	0	
66	$2 \cdot 3 \cdot 11$	4	3	
67	67	1	0	
68	$2^2 \cdot 17$	5	3	
69	$3 \cdot 23$	1	0	
70	$2 \cdot 5 \cdot 7$	4	3	
71	71	1	0	
72	$2^3 \cdot 3^2$	50	44	
73	73	1	0	
74	$2 \cdot 37$	2	1	
75	$3 \cdot 5^2$	3	1	
76	$2^2 \cdot 19$	4	2	
77	$7 \cdot 11$	1	0	
78	$2 \cdot 3 \cdot 13$	6	5	
79	79	1	0	
80	$2^4 \cdot 5$	52	47	
81	3^4	15	10	
82	$2 \cdot 41$	2	1	
83	83	1	0	
84	$2^2 \cdot 3 \cdot 7$	15	13	
85	$5 \cdot 17$	1	0	
86	$2 \cdot 43$	2	1	
87	$3 \cdot 29$	1	0	
88	$2^3 \cdot 11$	12	9	
89	89	1	0	
90	$2 \cdot 3^2 \cdot 5$	10	8	
91	$7 \cdot 13$	1	0	
92	$2^2 \cdot 23$	4	2	

Nombres de groupes d'ordre n : voir `https://oeis.org/A000001`
Nombres de groupes non-abélien d'ordre n : `https://oeis.org/A060689`

2. Géométrie affine

Référence : Audin, Chapitre 1.

I C'est quoi ?

La géométrie affine (réelle) est la géométrie que vous avez manipulé sans le savoir avant d'apprendre algèbre linéaire. La géométrie affine comme on va la définir dans ce chapitre, consiste : à utiliser l'algèbre linéaire pour construire rigoureusement (ou axiomatiser) la géométrie affine sur un corps quelconque.

Définition I.1 Un ensemble $\mathbb{A}$ est muni d'une structure d'*espace affine* par la donnée d'une action simplement transitive d'un espace vectoriel E sur $\mathbb{A}$. L'espace vectoriel E s'appelle *la direction* de $\mathbb{A}$.

On ne va pas noter cette action α, cela donnerait $\alpha(u)(A) = B$ très indigeste et loin de l'intuition. On va la noter $A + u$.

Il existe alors une application $\Theta : \mathbb{A} \times \mathbb{A} \to E$ donnée par $\Theta : (A,B) \mapsto \overrightarrow{AB}$ où $\overrightarrow{AB}$ est l'unique élément de E tel que $A + \overrightarrow{AB} = B$. L'application Θ vérifie :

1. Pour tout point $A \in \mathbb{A}$, l'application $\Theta_A : \mathbb{A} \to E$ donnée par $B \mapsto \overrightarrow{AB}$ est une bijection (vérification laissée en exo).
2. Pour tous points $A,B,C \in \mathbb{A}$, on a $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$ (Relation de Chasles).

   Démonstration. C'est la définition d'action :

   $$A + (\overrightarrow{AB} + \overrightarrow{BC}) = (A + \overrightarrow{AB}) + \overrightarrow{BC} = B + \overrightarrow{BC} = C$$

   Donc $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$. ∎

R Si A est un point d'un espace affine $\mathbb{A}$ dirigé par un espace vectoriel E et u un vecteur de E. L'unique point $B \in \mathbb{A}$ tel que $\overrightarrow{AB} = u$ est noté $B = A + u$; La relation de Chasles entraine que :

$$(A + u) + v = A + (u + v)$$

Les éléments de $\mathbb{A}$ sont appelés *points* par opposition aux éléments de E qui sont des vecteurs. On appelle *dimension* de $\mathbb{A}$ la dimension de l'espace vectoriel qui le dirige.

■ **Exemple 2.1** Les premiers exemples :

1. L'ensemble vide est un espace affine dirigé par n'importe quel espace vectoriel. On convient qu'il n'a pas de dimension.
2. Tout espace vectoriel E agit sur lui même par translation à gauche. Cette action est simplement transitive. Ainsi, tout espace vectoriel est muni d'une structure canonique d'espace affine. L'application $\Theta : E \times E \to E$ est donnée par $(u,v) \mapsto v-u$.
3. Si $\mathbb{A}_1, \mathbb{A}_2$ sont deux espaces affines dirigés par des k-espaces vectoriels E_1, E_2 alors $\mathbb{A}_1 \times \mathbb{A}_2$ est un espace affine dirigé par $E_1 \times E_2$, via l'application $\Theta : \mathbb{A}_1 \times \mathbb{A}_2 \times \mathbb{A}_1 \times \mathbb{A}_2 \to E_1 \times E_2$ donnée par : $(A_1, B_1, A_2, B_2) \mapsto (\overrightarrow{A_1B_1}, \overrightarrow{A_2B_2})$.

■

II Propriétés

Proposition II.1 Soient A, A', B, B' quatre points d'un espace affine, on a :

1. $\overrightarrow{AA} = \vec{0}$.
2. $\overrightarrow{AB} = -\overrightarrow{BA}$.
3. (Règle du parallélogramme) $\overrightarrow{AB} = \overrightarrow{A'B'}$ si et seulement si $\overrightarrow{AA'} = \overrightarrow{BB'}$. Dans ce cas, on dit que $ABB'A'$ est un parallélogramme.

Démonstration. On a $A + \vec{0} = A$ (définition d'une action) donc par unicité $\overrightarrow{AA} = \vec{0}$.

De $A + \overrightarrow{AB} = \alpha(\overrightarrow{AB}) \cdot A = B$, on en déduit que $B + -\overrightarrow{AB} = \alpha(-\overrightarrow{AB}) \cdot B = A$ donc $-\overrightarrow{AB} = \overrightarrow{BA}$. De la relation de Chasles :

$$\overrightarrow{AB} = \overrightarrow{AA'} + \overrightarrow{A'B'} + \overrightarrow{B'B}$$

On déduit que :

$$\overrightarrow{AB} = \overrightarrow{A'B'} \quad \Leftrightarrow \quad \overrightarrow{AA'} + \overrightarrow{B'B} = \vec{0}$$

■

Rappel : Pour tout point A d'un espace affine $\mathbb{A}$ dirigé par un espace vectoriel E, l'application $\Theta_A : \mathbb{A} \to E$ donnée par $M \mapsto \overrightarrow{AM}$ est une bijection.

Proposition II.2 Cette bijection permet de définir une structure d'espace vectoriel, noté $\mathbb{A}_A$, sur $\mathbb{A}$, i.e. on décrète que $M + N = Q$ lorsque $\overrightarrow{AM} + \overrightarrow{AN} = \overrightarrow{AQ}$.

R La structure ainsi définie dépend fortement du point base A choisi, celui-ci devenant en effet le zéro de l'espace vectoriel $\mathbb{A}_A$.

R L'espace vectoriel E possède une structure canonique d'espace affine. Alors qu'un espace affine $\mathbb{A}$ ne possède pas de structure naturelle d'espace vectoriel.

III Sous-espaces affines

Définition III.1 Un sous-ensemble $\mathcal{F}$ de $\mathbb{A}$ est un sous-espace affine s'il est vide ou s'il contient un point A tel que $\Theta_A(\mathcal{F})$ soit un sous-espace vectoriel de E.

Proposition III.1 Soit $\mathcal{F}$ un sous-espace affine de $\mathbb{A}$. Il existe un unique sous-espace vectoriel F de E tel que, pour tout point $B \in \mathcal{F}$, $\Theta_B(\mathcal{F}) = F$. On dit que le sous-espace affine $\mathcal{F}$ *est dirigé par* F, on note $\overrightarrow{\mathcal{F}} = F$.

Inversement, soit F un sous-espace vectoriel de E et A un point de $\mathbb{A}$. Il existe un unique sous-espace affine dirigé par F passant par A.

Démonstration. Soit $B \in \mathcal{F}$. Montrons que $\Theta_B(\mathcal{F}) = F$ (notation de la définition). On commence par montrer que $\Theta_B(\mathcal{F}) \subset F$. Soit $M \in \mathcal{F}$. Par définition :

$$\Theta_B(M) = \overrightarrow{BM} = \overrightarrow{BA} + \overrightarrow{AM} \in F$$

Ensuite, on montre que $F \subset \Theta_B(\mathcal{F})$. Soit $u \in F$. On sait qu'il existe un $M \in \mathcal{F}$ tel que $\overrightarrow{AM} = u$. On pose $N = M + \overrightarrow{AB}$ vérifions que $\Theta_B(N) = \overrightarrow{BN} = u$. On a :

$$\overrightarrow{BN} = \overrightarrow{BA} + \overrightarrow{AM} + \overrightarrow{MN} = \overrightarrow{BA} + \overrightarrow{AM} + \overrightarrow{AB}$$

Pour la seconde partie (laissée en exo), vérifier que :

$$\mathcal{F} = \{M \in \mathbb{A} \,|\, \overrightarrow{AM} \in F\}$$

est un sous-espace affine. Il est clair que c'est le seul possible. ■

R Si M et N sont deux points de $\mathcal{F}$ alors $\overrightarrow{MN} \in F$.

La *dimension* d'un sous-espace affine non vide est la dimension de sa direction.

■ **Exemple 2.2**

1. Un espace affine de dimension 0 est constitué d'un unique point. Tous les points d'un espace affine sont des sous-espaces affines de dimension 0.
2. On appelle *droite*, *plan* les sous-espaces affines de dimension 1, 2.
3. Si $f : E \to F$ est une application linéaire alors $f^{-1}(v)$ est un sous-espace affine de E, muni de sa structure naturelle d'espace affine, dirigé par $\ker f$.
4. Plus généralement, les sous-espaces affines d'un espace vectoriel E sont les sous-espaces de la forme $F + u_0$ où F est un sous-espace vectoriel et u_0 un vecteur. Les sous-espaces vectoriels sont les sous-espaces affines contenant 0.

■

R On peut définir la notion de sous-espace affine engendré par une partie comme on définit la notion de sous-espace vectoriel engendré, sous-groupe engendré, etc... aka intersection des sous-machins contenant la partie en question.

.....Fin du cours 4.....

IV Parallélisme

Définition IV.1 Deux sous-espaces affines $\mathcal{F}, \mathcal{G}$ sont *parallèles*, noté $\mathcal{F} /\!\!/ \mathcal{G}$ s'ils ont la même direction.

R [Exo du TD]

1. Deux sous-espaces affines peuvent être disjoints sans être parallèles.
2. Néanmoins, dans un plan affine, deux droites affines sont parallèles si et seulement si elles sont disjointes.
3. Deux sous-espaces parallèles sont disjoints ou égaux.
4. Par tout point d'un espace affine, il passe une unique droite parallèle à une droite donnée.

Démonstration. Le premier point est évident, prendre ses bras !

Pour le second point, supposons que $\mathcal{D}$ et $\mathcal{D}'$ ne sont pas parallèles, alors les droites vectorielles D et D' vérifient : $D \neq D'$ mais on est dans un plan donc :

$$D \cap D' = \{0\} \qquad D + D' = P$$

On veut montrer que $\mathcal{D} \cap \mathcal{D}' \neq \varnothing$. On se donne $A \in \mathcal{D}$ et $A' \in \mathcal{D}'$. On cherche un $u \in D$ et $v \in D'$ tel que :

$$A + u = B + v$$

qui se réécrit :

$$A = B + (v - u) \quad \Leftrightarrow \overrightarrow{BA} = v - u$$

De tels u, v existent bien car $D + D' = P$. Ils sont même unique puisque $D \cap D' = \{0\}$. ■

Proposition IV.1 Soient $\mathcal{F}$ et $\mathcal{G}$ deux sous-espaces affines d'un espace affine $\mathbb{A}$, dirigés respectivement par F et G. On suppose que $F + G = E$. Alors tout sous-espace parallèle à $\mathcal{G}$ rencontre $\mathcal{F}$. De plus, cette intersection est un singleton si $F \cap G = \{0\}$.

Démonstration. Exo du TD ■

V Application affine

1. Définition

Définition V.1 Une application $\varphi : \mathcal{E} \to \mathcal{F}$ entre deux espaces affines est dite *affine* lorsqu'il existe un point $O \in \mathcal{E}$, et une application linéaire $f : E \to F$ tel que :

$$\forall M \in \mathcal{E}, \quad \overrightarrow{\varphi(O)\varphi(M)} = f(\overrightarrow{OM})$$

L'application f ne dépend pas du choix du point O. On dit que f est le *linéarisé* de φ et on la note $f = \overrightarrow{\varphi}$.

Démonstration. Un tel f est unique puisque :

$$f(u) = \overrightarrow{\varphi(O)\varphi(O+u)}.$$

Soit A un point, on a :

$$\overrightarrow{\varphi(A)\varphi(M)} = \overrightarrow{\varphi(A)\varphi(O)} + \overrightarrow{\varphi(O)\varphi(M)} = f(\overrightarrow{AO}) + f(\overrightarrow{OM}) = f(\overrightarrow{AM})$$

■

■ **Exemple 2.3**

- Les applications constantes sont affines, $f = 0$.
- Si $\mathcal{E} = \mathcal{F} = k$ alors les applications affines sont les applications $x \mapsto ax + b$ avec $a, b \in k$.
- Si $\mathcal{E} = k^d$ et $\mathcal{F} = k^e$ alors les applications affines sont les applications $x \mapsto Ax + B$ avec $A \in \mathrm{M}_{e,d}(k)$ et $B \in k^e$.

  Démonstration. On note $B = \varphi(0)$ et A la matrice de f dans la base canonique. On a alors :
  $$\overrightarrow{\varphi(x)\varphi(0)} = Ax \quad \Leftrightarrow \quad \varphi(x) = Ax + \varphi(0) = Ax + B$$
  La réciproque est évidente. ■

- Si $\mathcal{E} = E$ et $\mathcal{F} = F$, une application $\varphi : E \to F$ est une application affine si et seulement s'il existe une application linéaire $f : E \to F$ et un vecteur $v_0 \in F$ tel que $\varphi(u) = f(u) + v_0$.

  Démonstration. Prendre $v_0 = \varphi(0)$. ■

- Les applications linéaires sont donc les applications affines qui envoient 0 sur 0.

■

Proposition V.1 Soient $\mathcal{F}$ et $\mathcal{G}$ deux sous-espaces affines d'un espace affine $\mathbb{A}$, dirigés respectivement par F et G. On suppose que $F \oplus G = E$. Pour tout $x \in \mathbb{A}$, on note $\pi(x) \in \mathcal{F}$ le point d'intersection de $\mathcal{F}$ et de l'unique sous-espace affine parallèle à $\mathcal{G}$ contenant x. L'application $\pi(x)$ est affine de linéarisé la projection vectoriel sur F parallèlement à G.

Démonstration. Soit A l'unique point de $\mathcal{F} \cap \mathcal{G}$. On décide que A est l'origine de $\mathcal{E}$, l'espace affine $\mathcal{E}$ devient donc un espace vectoriel, les espaces affines $\mathcal{F}$ et $\mathcal{G}$ deviennent des sous-espaces vectoriels et l'application π devient alors la projection linéaire sur $\mathcal{F}$ parallèlement à $\mathcal{G}$. ■

2. Translations - Homothéties

Définition V.2 Soit $\varphi : \mathcal{E} \to \mathcal{E}$ une application affine. On dit que φ est une *translation* lorsque $\overrightarrow{\varphi} = \mathrm{Id}$.

R Soit φ une translation. On a $\overrightarrow{\varphi(A)\varphi(B)} = \overrightarrow{AB}$ pour tous $A, B \in \mathcal{E}$. La règle du parallélogramme entraine que $\overrightarrow{A\varphi(A)} = \overrightarrow{B\varphi(B)}$ pour tous $A, B \in \mathcal{E}$. Autrement dit, le vecteur $\overrightarrow{M\varphi(M)}$ est constant égale à u. On dit que φ est la *translation* de vecteur u et on la note t_u.

Définition V.3 Soient O un point et $\lambda \in k$ un scalaire. L'application φ définie par $\overrightarrow{O\varphi(M)} = \lambda\overrightarrow{OM}$ est affine. L'application linéaire associée est l'homothétie de centre O et de rapport λ. Le point O est fixé par φ. On appelle φ *l'homothétie de centre O et de rapport λ*, on la note $h_{O,\lambda}$.

3. Propriétés

Proposition V.2
- L'image d'un sous-espace affine par une application affine est un sous-espace affine.
- Toute application affine envoie trois points alignés sur trois points alignés.
- L'image inverse d'un sous-espace affine par une application affine est un sous-espace affine.

Démonstration. Exo du TD. ■

Proposition V.3 La composée de deux applications affines $\varphi : \mathcal{E} \to \mathcal{F}$ et $\psi : \mathcal{F} \to \mathcal{G}$est une application affine et $\overrightarrow{\psi \circ \varphi} = \overrightarrow{\psi} \circ \overrightarrow{\varphi}$.

Démonstration. Par définition, on a :

$$\forall M, N \in \mathcal{E}, \quad \overrightarrow{\varphi(M)\varphi(N)} = \overrightarrow{\varphi}(\overrightarrow{MN})$$
$$\forall M, N \in \mathcal{F}, \quad \overrightarrow{\psi(M)\varphi(N)} = \overrightarrow{\psi}(\overrightarrow{MN})$$

On a donc :

$$\begin{aligned} \overrightarrow{\psi \circ \varphi(M)\psi \circ \varphi(N)} &= \overrightarrow{\psi(\varphi(M))\psi(\varphi(N))} \\ &= \overrightarrow{\psi}\overrightarrow{\varphi(M)\varphi(N)} \\ &= \overrightarrow{\psi} \circ \overrightarrow{\varphi}(\overrightarrow{MN}) \end{aligned}$$

■

VI Groupe affine

Proposition VI.1 Une application affine est bijective si et seulement si sa linéarisé est bijective. Dans ce cas, φ^{-1} est une application affine de linéarisé $\overrightarrow{\varphi}^{-1}$. En formule, $\overrightarrow{\varphi^{-1}} = \overrightarrow{\varphi}^{-1}$.

Démonstration. Par définition, on a que :

$$\varphi(X) = \varphi(Y) \quad \Leftrightarrow \quad f(\overrightarrow{XY}) = \overrightarrow{0}$$

Donc φ injective est équivalent à f injective. On se donne un point O d'image $O' = \varphi(O)$. Soit M' un point quelconque alors l'équation suivante en $M \in \mathcal{E}$ devient :

$$\varphi(M) = M' \quad \Leftrightarrow \quad f(\overrightarrow{OM}) = \overrightarrow{O'M'}$$

Ainsi l'injectivité/surjectivité de φ et f sont équivalentes.

Supposons φ bijective alors on applique la définition d'application affine à $\varphi = \varphi$ et $A = \varphi^{-1}(A)$, idem B, on obtient :

$$\overrightarrow{\varphi(\varphi^{-1}(A))\varphi(\varphi^{-1}(B))} = \overrightarrow{\varphi}(\overrightarrow{\varphi^{-1}(A)\varphi^{-1}(B)})$$

On applique $\overrightarrow{\varphi}^{-1}$, on obtient :

$$\overrightarrow{\varphi}^{-1}(\overrightarrow{AB}) = \overrightarrow{\varphi^{-1}(A)\varphi^{-1}(B)}$$

■

Corollaire VI.2 Les bijections affines de $\mathcal{E}$ dans lui-même forme un groupe, le *groupe affine*, noté $\mathrm{GA}(\mathcal{E})$.

Proposition VI.3 L'application linéarisé du groupe affine vers le groupe linéaire est un morphisme surjectif, de noyau le groupe des translations $\mathrm{T}(\mathcal{E}) \simeq E$. La suite exacte ainsi définie est scindée. On a le produit semi-direct :

$$\mathrm{GA}(\mathcal{E}) \simeq E \rtimes \mathrm{GL}(E)$$

Démonstration. La première phrase est claire. On peut supposer que $\mathcal{E} = E$ en choissiant une origine O. Via, ce choix on va montrer que

$$\mathrm{GA}(E) = E \rtimes \mathrm{GL}(E) \qquad \text{produit semi-direct interne}$$

Il reste à montrer que :

$$\langle \mathrm{T}(E), \mathrm{GL}(E) \rangle = \mathrm{GA}(E) \quad \text{et} \quad \mathrm{T}(E) \cap \mathrm{GL}(E) = 1$$

Le second point est trivial, en effet le linéarisé d'une application linéaire est elle-même. Le premier point n'est pas difficile. Soit $u = \overrightarrow{O\varphi(O)}$ alors l'application affine $t_{-u} \circ \varphi$ envoie O sur O, elle est donc linéaire. ■

Corollaire VI.4 Étant donné un point $O \in \mathcal{E}$, toute application affine $\varphi : \mathcal{E} \to \mathcal{E}$ s'écrit de façon unique sous la forme :

$$\varphi = t_u \circ \psi = \psi \circ t_v$$

où ψ fixe O. (On a $u = \vec{\psi}(v)$).

VII Le théorème de Thalès

Rapport de longueur

Définition VII.1 Soient A, B, C trois points alignés. Il existe un unique λ tel que $\overrightarrow{AB} = \lambda \overrightarrow{AC}$. On note $\lambda = \frac{\overline{AB}}{\overline{AC}}$ et l'appelle le rapport algébrique. Attention, la longueur algébrique $\overline{AB}$ n'a pas de sens en géométrie affine. Pour lui donner un sens (facilement), il faudrait que $k = \mathbb{R}$ et avoir choisit un produit scalaire. Autrement dit, faire de la géométrie euclidienne.

Théorème de Thalès

Théorème VII.1 — Théorème de Thalès, version général. Soient d, d', d'' trois droites parallèles distinctes d'un plan affine. Soient $\mathcal{D}_1, \mathcal{D}_2$ deux droites non-parallèles à d. On note pour $i = 1, 2$, $A_i = \mathcal{D}_i \cap d$, $A_i' = \mathcal{D}_i \cap d'$ et $A_i'' = \mathcal{D}_i \cap d''$. Alors on a :

$$\frac{\overline{A_1A_1''}}{\overline{A_1A_1'}} = \frac{\overline{A_2A_2''}}{\overline{A_2A_2'}}$$

Réciproquement, un point $B \in \mathcal{D}_1$ vérifie l'égalité :

$$\frac{\overline{A_1B}}{\overline{A_1A_1'}} = \frac{\overline{A_2A_2''}}{\overline{A_2A_2'}}$$

alors $B = A_1''$.

R Le théorème de Thalès exprime que les projections sont des applications affines.

Démonstration. On note π la projection sur $\mathcal{D}_2$ parallèlement à d, c'est une application affine. On note p sa linéarisé. On a :

$$\pi(A_1) = A_2 \qquad \pi(A_1') = A_2' \qquad \pi(A_1'') = A_2''$$

On note λ l'unique scalaire tel que $\overrightarrow{A_1A_1''} = \lambda\overrightarrow{A_1A_1'}$, autrement dit $\lambda = \frac{\overline{A_1A_1''}}{\overline{A_1A_1'}}$. On en déduit, par linéarité de p que :

$$p(\overrightarrow{A_1A_1''}) = \lambda p(\overrightarrow{A_1A_1'}) \quad \text{autrement dit} \quad \overrightarrow{A_2A_2''} = \lambda\overrightarrow{A_2A_2'} \quad \text{autrement dit} \quad \frac{\overline{A_2A_2''}}{\overline{A_2A_2'}} = \lambda$$

Enfin, l'hypothèse sur B :

$$\frac{\overline{A_1B}}{\overline{A_1A_1'}} = \frac{\overline{A_2A_2''}}{\overline{A_2A_2'}} = \lambda \quad \text{se lit} \quad \overrightarrow{A_1B} = \lambda\overrightarrow{A_1A_1'} \quad \text{d'où} \quad B = A_1''$$

■

Théorème VII.2 — Théorème de Thalès, version 3ème. Soient $\mathcal{D}_1, \mathcal{D}_2$ deux droites d'un plan affine sécantes en A, d et d' deux droites parallèles coupant $\mathcal{D}_i$ en A_i, A_i' distincts de A. Alors :

$$\frac{\overline{AA_1}}{\overline{AA_1'}} = \frac{\overline{AA_2}}{\overline{AA_2'}} = \frac{\overline{A_1A_2}}{\overline{A_1'A_2'}}$$

Démonstration. Ajouter une droite d'' parallèle à d et passant par A pour obtenir la première égalité. Déduire de cette égalité que l'homothétie de centre A et de rapport $\frac{\overline{AA_1}}{\overline{AA_1'}}$ envoie A_1 sur A_1' et A_2 sur A_2'... ■

Pour aller plus loin, lire Audin chapitre 1 (Géométrie Affine), voir chap. 2 (Géométrie Euclidienne : généralités), 3 (Géométrie Euclidienne plane) et 5. (Géométrie Euclidienne espace).

La section suivante n'est pas faite en cours.
On dit rien sur les barycentres et les repères
Si $\mathcal{E} = k^d$ alors on note $\mathrm{GA}(k^d) = \mathrm{GA}_d(k)$.

Corollaire VII.3 Si k est le corps fini a q éléments alors le cardinal de $\mathrm{GA}_d(k)$ est $\#\mathrm{GL}_d(k) \cdot q^d$. En particulier :

$$\#\mathrm{GA}_1(\mathbb{F}_q) = (q-1)q$$

$$\#\mathrm{GA}_1(\mathbb{F}_2) = 2 \quad \#\mathrm{GA}_1(\mathbb{F}_3) = 6 \quad \#\mathrm{GA}_1(\mathbb{F}_4) = 12 \quad \#\mathrm{GA}_1(\mathbb{F}_5) = 20$$

Corollaire VII.4 Soient $p < q$ deux nombres premiers avec $p|q-1$. L'unique groupe non-abélien d'ordre pq est isomorphe à l'unique, à conjugaison près sous-groupe d'ordre pq de $\mathrm{GA}_1(\mathbb{F}_q)$.

Théorème de Pappus

Théorème VII.5 Soient A, B, C trois points d'une droite $\mathcal{D}$ et A', B', C' trois points d'une droite $\mathcal{D}' \neq \mathcal{D}$. Si la droite $AB' \parallel A'B$ et $BC' \parallel B'C$ alors $AC' \parallel A'C$.

Démonstration. On commence par supposer que $\mathcal{D}$ et $\mathcal{D}'$ sont concourantes en O. On note φ l'homothétie de centre O qui envoie A sur B et ψ celle qui envoie B sur C. Les hypothèses et le fait qu'une homothétie envoie une droite sur une droite parallèle montre que :

$$\varphi(B') = A' \qquad \text{et} \qquad \psi(C') = B'$$

Enfin, deux homothéties de même centre commutent par conséquent :

$$\varphi \circ \psi(C') = A' \qquad \text{et} \qquad \varphi \circ \psi(A) = \psi \circ \varphi(A) = C$$

La conclusion suit.

Pour faire le cas $\mathcal{D} \parallel \mathcal{D}'$ deux solutions : Changer les homothéties du raisonnement précédent en translation (exo) ou attendre un argument projectif qui montrera que ce cas est conséquence du premier. ■

Théorème de Desargues

Théorème VII.6 Soient ABC et $A'B'C'$ deux triangles sans sommet commun et à côtés respectivement parallèles. Alors les droites AA', BB' et CC' sont concourantes ou parallèles.

Démonstration. ■

3. Géométrie projective

Encouragement fort et à répéter à lire le Audin, Chapitre 1 (Géométrie Affine) et Chapitre 6 (Géométrie Projective). Le livre contient plus que ce cours. En particulier, ce cours ne parle pas de repère affine/projectif, de coordonnées, de barycentre, etc...

I Espaces projectifs : c'est quoi ?

1. C'est quoi ?

Soient k un corps et E un k-espace vectoriel, *l'espace projectif* $\mathbb{P}(E)$ *sur* E est l'ensemble des droites vectorielles de E, en d'autres termes l'ensemble des classes d'équivalence de $E \setminus \{0\}$ sous la relation d'équivalence de colinéarité :

$$u \simeq v \quad \Leftrightarrow \quad \exists \lambda \in k^*, u = \lambda v$$

Autrement, le quotient de $E \setminus \{0\}$ sous l'action de k^* par homothétie. On notera $\pi : E \setminus \{0\} \to \mathbb{P}(E)$, $u \mapsto [u]$ la projection de l'espace vectoriel vers l'espace projectif.

La *dimension* de $\mathbb{P}(E)$ est $\dim E - 1$. Si $E = \{0\}$ alors $\mathbb{P}(E) = \varnothing$. Si $\dim E = 1$ alors $\mathbb{P}(E)$ est réduit à un élément. Si $\dim E = 2$ (resp. $= 3$) alors $\mathbb{P}(E)$ est une *droite projective* (resp. *un plan projectif*)

Lorsque $E = k^{n+1}$, on notera $\mathbb{P}(E) = \mathbb{P}(k^{n+1}) = \mathbb{P}^n(k) = k\mathbb{P}^n$, l'espace projectif standard de dimension n sur k.

.....Fin du cours 5.....

Exam 1 : vendredi 16 octobre

.....Fin du cours 6.....

2. Topologie lorsque $k = \mathbb{R}$ ou $\mathbb{C}$

Lorsque $k = \mathbb{R}$ ou $\mathbb{C}$, on munit $\mathbb{P}(E)$ de la topologie quotient. C'est à dire de la topologie la plus fine qui rend l'application π continue. Autrement dit, une partie $\mathcal{U} \subset \mathbb{P}(E)$ est ouverte si et seulement si $\pi^{-1}(\mathcal{U})$ est ouverte.

Exercice 3.1 Montrer que l'application π est ouverte (i.e. l'image d'un ouvert est un ouvert). *Ind. Utiliser que la relation d'équivalence définissant $\mathbb{P}(E)$ est donnée par une action de groupe.* ∎

En pratique, une suite de droites $\ell_n \to \ell_\infty$ si et seulement s'ils existent une suite de vecteurs $0 \neq u_n \in \ell_n$ et un vecteur $0 \neq u_\infty \in \ell_\infty$ tel que $u_n \to u_\infty$.

Exercice 3.2

1. Montrer que l'application $\pi : \mathbb{S}^d \to \mathbb{RP}^d$ induit un homéomorphisme entre $\mathbb{S}^d/\{\pm \mathrm{Id}\}$ et $\mathbb{RP}^d$.
2. En déduire que $\mathbb{RP}^1$ est homéomorphe à un cercle.
3. Trouver un recollement des côtés d'un carré dont l'espace quotient est $\mathbb{RP}^2$.
4. Trouver un ouvert de $\mathbb{RP}^2$ homéomorphe à un ruban de Moëbius.
5. Montrer que l'application $\pi : \mathbb{S}^{2d+1} \to \mathbb{CP}^d$ induit un homéomorphisme entre $\mathbb{S}^{2d+1}/\mathbb{S}^1$ et $\mathbb{CP}^d$.

∎

Lemma I.1 Soit $f : X \to Y$ une bijection continue entre deux espaces topologiques. Si X est compact alors f est un homéo.

Exercice 3.3 Montrer que $\#k\mathbb{P}^d = q^d + q^{d-1} + \cdots + 1$, si k est le corps fini de cardinal q. ∎

II Sous-espaces projectifs

Définition II.1 Une partie V de $\mathbb{P}(E)$ est un *sous-espace projectif* si elle est l'image d'un sous-espace vectoriel non-trivial F de E via π.

On a donc une bijection entre les sous-espaces vectoriels de dimension $k+1$ de E et les sous-espaces projectifs de dimension k de $\mathbb{P}(E)$.

Proposition II.1 Soient V et W deux sous-espaces projectifs de $\mathbb{P}(E)$.

1. Si leurs dimensions vérifient l'inégalité :
$$\dim V + \dim W \geqslant \dim \mathbb{P}(E)$$
alors $V \cap W \neq \varnothing$.
2. En particulier, deux droites d'un plan projectif sont égales ou concourantes.
3. Soit H un hyperplan projectif de $\mathbb{P}(E)$ et soit m un point hors de H. Toute droite passant par m rencontre H en et un seul point.

Démonstration. Si X est un sous-espace projectif, alors on note $\overline{X}$ le sous-espace vectoriel tel que $\pi(\overline{X} \setminus \{0\}) = X$. Il est bien connu que :
$$\dim \overline{V} + \dim \overline{W} = \dim(\overline{V} + \overline{W}) + \dim \overline{V} \cap \overline{W}$$

On a les inégalités suivantes :

1. $\dim \overline{V} + \dim \overline{W} = \dim V + \dim W + 2 \geqslant d + 2$.
2. $\dim(\overline{V} + \overline{W}) \leqslant d + 1$

Par conséquent, $\dim \overline{V} \cap \overline{W} \geqslant 1$ et donc $\dim V \cap W \geqslant 0$. L'énoncé sur les droites d'un plan projectif est une conséquence évidente du premier point. Pour montrer le troisième point, il suffit de s'apercevoir que sous les hypothèses de 3., on a $\dim(\overline{V} + \overline{W}) = d + 1$. On en tire que $\dim(\overline{V} \cap \overline{W}) = 1$, d'où la conclusion. ■

R Si on applique le point 2. dans le cas d'un corps fini, disons le corps fini à 5 éléments. On obtient qu'il existe un sous-ensemble [1] $\{A_1, \ldots, A_n\}$ de $\mathcal{P}(k\mathbb{P}^2)$ constitué uniquement de sous-ensembles de cardinal 6 tel que pour toute paire d'éléments distincts A_i et A_j, on a $\#A_i \cap A_j = 1$. Remarque, ici $n = 5^2 + 5 + 1 = 31$. Application : le jeu dooble. Voir TD.

R On peut définir comme dans le cas vectoriel, la notion de sous-espace projectif engendré par une partie.

III Liaison affine/projectif

On va voir que la géométrie projective contient la géométrie affine, au sens où l'espace projectif de dimension n peut-être vu comme un "complété" de l'espace affine de dimension n.

1. La droite projective

On suppose que E est un espace vectoriel de dimension 2, on veut décrire la droite projective $\mathbb{P}(E)$ (= l'ensemble des droites vectorielles de E).

On choisit une base (e_1, e_2) de E, toutes les droites vectorielles de E ont un unique vecteur directeur de coordonnées $(x, 1)$ sauf la droite $d_\infty = \{y = 0\}$. Autrement dit, toutes les droites vectorielles du plan rencontrent la droite affine horizontale $\{y = 1\}$ sauf la droite vectorielle horizontale $\{y = 0\}$.

Il existe donc une bijection entre la droite projective privé du point d_∞ et la droite affine $\{y = 1\}$. On peut donc identifier la droite affine à la droite projective privée d'un point.

Inversement, on peut considérer qu'on a obtenu la droite projective en ajoutant un point à la droite affine. Il est traditionnel d'appeler ce point : *point à l'infini*. La bijection est donnée par :

$$\begin{array}{ccc} \{y = 1\} \cup \{\infty\} & \to & \mathbb{P}(E) \\ (x, 1) & \mapsto & \text{la droite vectorielle engendrée par } (x, 1) \\ \infty & \mapsto & \text{la droite vectorielle engendrée par } (1, 0) \end{array}$$

On a aussi la bijection :

$$\begin{array}{cccc} \hat{k} := & k \cup \{\infty\} & \to & \mathbb{P}(E) \\ & x & \mapsto & \text{la droite vectorielle engendrée par } (x, 1) \\ & \infty & \mapsto & \text{la droite vectorielle engendrée par } (1, 0) \end{array}$$

Lorsque $k = \mathbb{R}$ ou $\mathbb{C}$, et que l'on munit l'espace de gauche de la topologie de *compactifié d'Alexandrov*, cette bijection est un homéomorphisme.

1. En clair, les droites de $\mathcal{P}(k\mathbb{P}^2)$

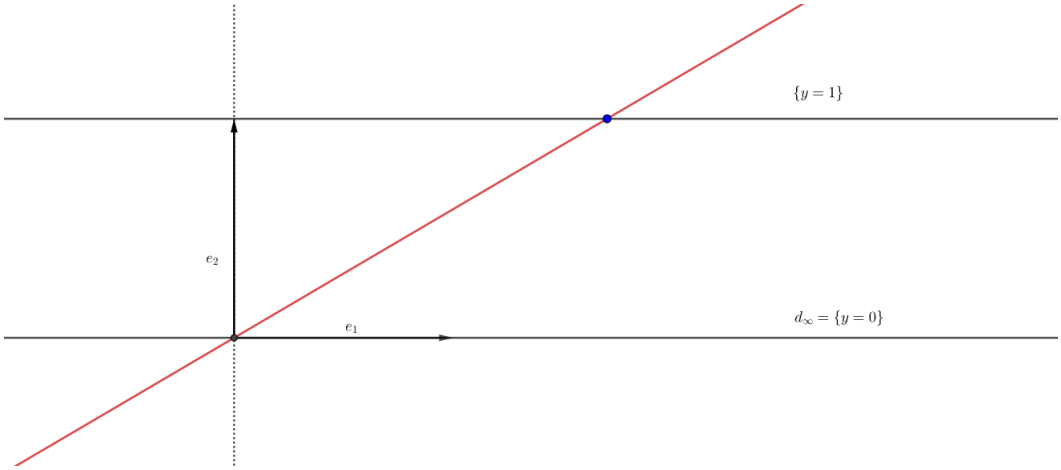

FIGURE 3.1 – Liaison affine – projectif en dimension 1

R À l'aide d'un bon dessin, on peut montrer ou redémontrer que $\mathbb{RP}^1 \simeq \mathbb{S}^1$.

R La compactification d'Alexandrov d'un espace topologique (localement compact) X est l'espace topologique $\hat{X} = X \cup \{\infty\}$, où une base d'ouverts du point ∞ est donné par les complémentaires des compacts de X. Cette procédure est très pratique. L'exercice classique consiste à montrer que $\hat{\mathbb{R}^d} \simeq \mathbb{S}^d$, pour cela on utilise généralement la projection stéréographique.

2. Le plan projectif

On procède de la même façon avec un espace E de dimension 3 : on choisit une base et on note $\mathcal{F} = \{z = 1\}$ l'hyperplan horizontal de hauteur 1, F l'espace vectoriel qui le dirige. Une droite vectorielle ℓ de E rencontre $\mathcal{F}$ en un unique point sauf si elle est incluse dans F.

On a donc une bijection entre $\mathbb{P}(E) \setminus \mathbb{P}(F)$ et $\mathcal{F}$. Inversement, on peut considérer que le plan projectif $\mathbb{P}(E)$ complète le plan affine $\mathcal{F}$ en lui ajoutant une *droite à l'infini* : la droite $\mathbb{P}(F)$.

3. Le cas général : complétion projective d'un espace affine

Définition III.1 Soit $\mathcal{F}$ un espace affine de direction F. L'espace projectif $\mathbb{P}(F \times k)$ est le *complété projectif de* $\mathcal{F}$ et $\mathbb{P}(F \times \{0\})$ est *l'hyperplan à l'infini* de $\mathcal{F}$.

Attention, c'est une construction canonique. On plonge $\mathcal{F}$ dans $F \times k$ comme l'hyperplan à hauteur 1. Pour cela, on choisit une origine o sur $\mathcal{F}$ et on considère l'injection $\mathcal{F} \to F \times \mathbb{R}$, $m \mapsto (\overrightarrow{om}, 1)$. L'hyperplan $\{x_{n+1} = 0\}$ de $F \times k$ s'identifie avec F.

Toute droite vectorielle de $F \times k$ non contenu dans F rencontre $\mathcal{F}$ en un et un seul point. On a donc obtenu une bijection entre $\mathcal{F}$ et $\mathbb{P}(F \times k) \setminus \mathbb{P}(F \times \{0\})$.

R L'hyperplan à l'infini $\mathbb{P}(F \times \{0\})$ n'intersecte pas $\mathcal{F}$ et est constitué des directions des droites affines de $\mathcal{F}$.

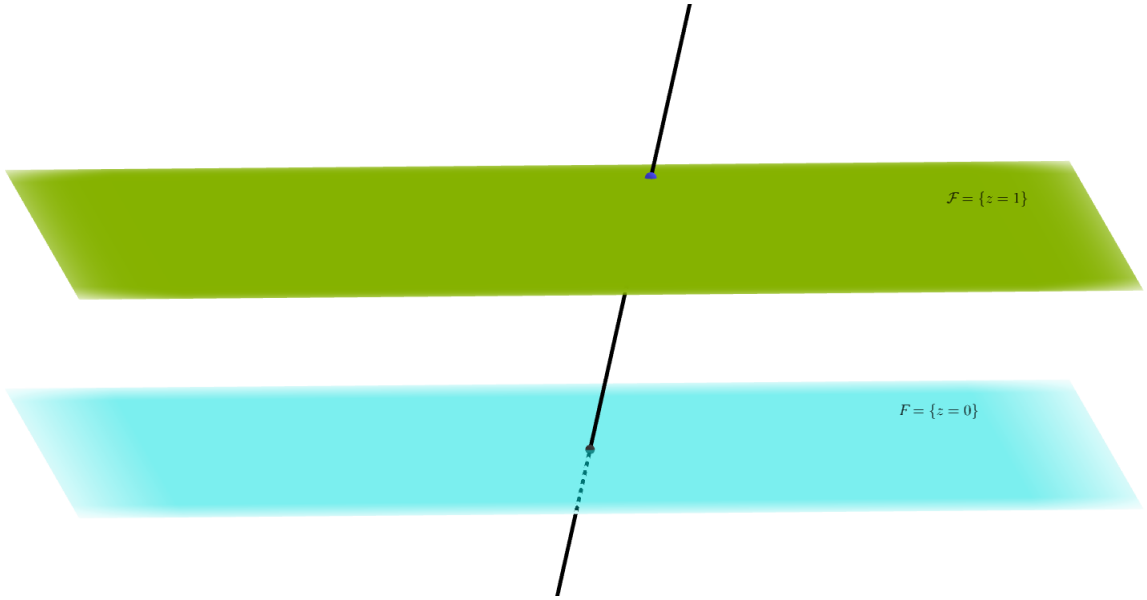

FIGURE 3.2 – Liaison affine – projectif en dimension 2

4. Droites affines, droites projectives

Soit $\mathcal{F}$ un espace affine et $\mathbb{P}(F \times k)$ son complété projectif. Soit $\mathcal{D}$ une droite affine de $\mathcal{F}$. Il existe un unique plan vectoriel de $F \times k$ qui contient $\mathcal{D}$: le plan engendré par $\mathcal{D}$. On le note $\mathcal{P}_{\mathcal{D}}$, il définit une droite projective d de $\mathbb{P}(F \times k)$. On note :

$$\underbrace{\infty_{\mathcal{D}}}_{\in \mathbb{P}(F \times k)} := \underbrace{D}_{\text{droite vectorielle de } F \times k}$$

On voit ainsi $d = \mathcal{D} \cup \{\infty_{\mathcal{D}}\}$ est le complété projectif de la droite affine $\mathcal{D}$.

R On a une bijection entre les droites affines de $\mathcal{F}$ et les droites projectives de son complété qui ne sont pas dans l'hyperplan à l'infini.

5. Intersections de droites dans le plan

Soit $\mathcal{F}$ un plan affine de direction F. Le complété projectif $\mathbb{P}(F \times k)$ de $\mathcal{F}$ est la réunion de $\mathcal{F}$ et de la droite projective $\mathbb{P}(F \times \{0\})$: la droite à l'infini de $\mathcal{F}$.

La liste des droites projectives de $\mathbb{P}(F \times k)$ peut éclairer la compréhension de tout ce bazar. Les droites projectives de $\mathbb{P}(F \times k)$ correspondent au plan vectoriel de l'espace vectoriel $F \times k$ de dimension 3. Il y a la droite à l'infini : $\mathbb{P}(F)$ et les droites projectives qui viennent de droites affines auxquelles on a ajouté un point. Si $\mathcal{D}$ est un droite affine de direction D, alors on note $\infty_{\mathcal{D}} = D$ ce point.

R La droite à l'infini de $\mathbb{P}(F \times k)$ est $\mathbb{P}(F \times \{0\})$ l'ensemble des droites vectorielles D de F, c'est à dire l'ensemble des directions des droites affines de $\mathcal{F}$. Chaque point de la droite à l'infini est une direction de droites parallèles dans $\mathcal{F}$.

On sait que deux droites projectives d'un plan projectif se rencontre en un point. Revenons sur cet énoncé pour le complété projectif d'un plan affine.

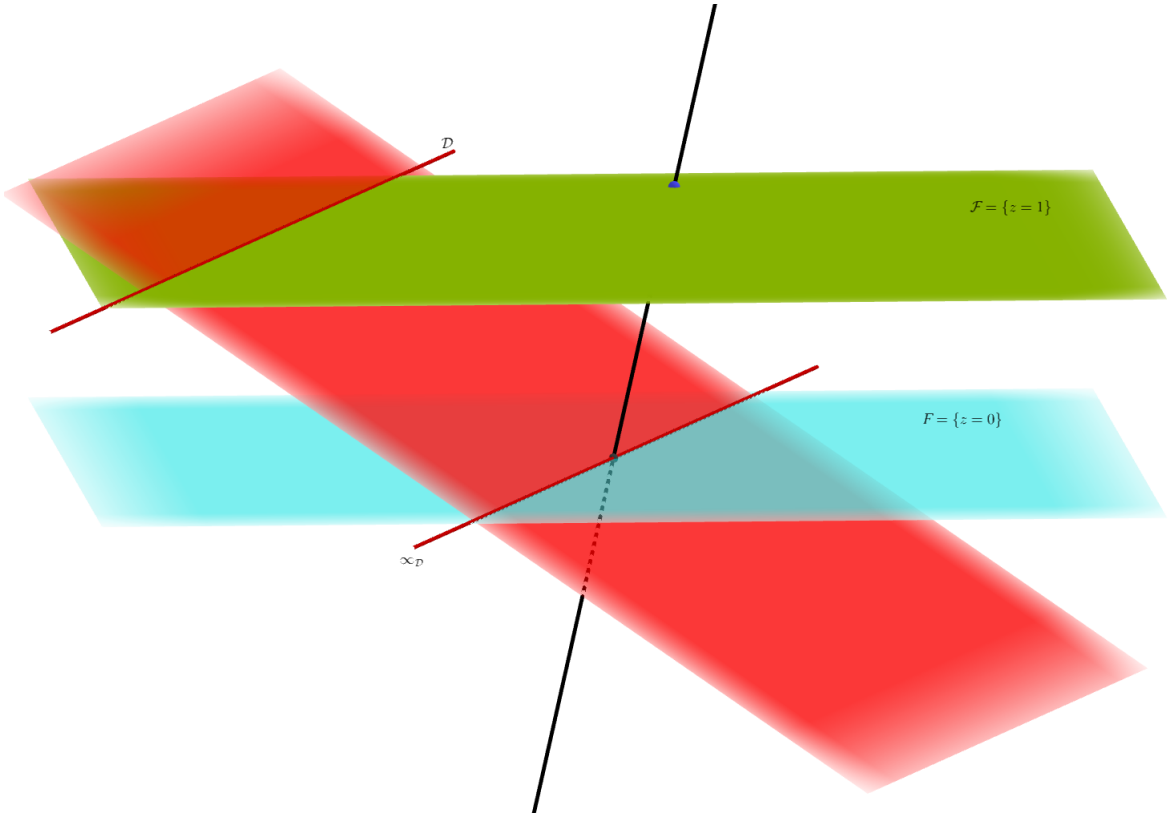

FIGURE 3.3 – La complétion d'une droite affine dans un plan affine dans un plan projectif

- La droite à l'infini et la droite projective d provenant de $\mathcal{D}$ se rencontre au point $\infty_{\mathcal{D}}$. En vectoriel, l'intersection du plan $F \times \{0\}$ et du plan engendré par $\mathcal{D}$ est la direction de $\mathcal{D}$, autrement dit $\infty_{\mathcal{D}}$.
- Deux droites affines $\mathcal{D}, \mathcal{D}'$ non-parallèles se rencontrent en M. En vectoriel, les plans $\mathcal{P}_{\mathcal{D}}$ et $\mathcal{P}_{\mathcal{D}'}$ se rencontrent en la droite OM, qu'on assimile au point M dans $\mathbb{P}(F \times k)$.
- Deux droites projectives d, d' provenant de deux droites affines $\mathcal{D}, \mathcal{D}'$ parallèles se rencontrent en $\infty_{\mathcal{D}} = \infty_{\mathcal{D}'}$, où D est leur direction commune. En vectoriel, l'intersection du plan $\mathcal{P}_{\mathcal{D}}$ et du plan $\mathcal{P}_{\mathcal{D}'}$ est la droite $D = \infty_{\mathcal{D}} = \infty_{\mathcal{D}'}$.

6. Choix de l'infini

Dans un espace projectif, il n'y a pas d'hyperplan à l'infini. Autrement dit, on peut choisir tous hyperplans comme étant l'hyperplan à l'infini. En d'autres termes, choissisons un hyperplan F de E, retirons $\mathbb{P}(F)$ à $\mathbb{P}(E)$, le résultat est un espace affine $\mathcal{F}$ dirigé par F dont l'hyperplan à l'infini est $\mathbb{P}(F)$.

7. Le Théorème de Pappus

Théorème III.1 — Théorème de Pappus, $\simeq 300$ apr JC. Soient D, D' deux droites d'un plan projectif. Soient a, b, c trois points de D et a', b', c' trois points de D'. Soient α, β, γ les points d'intersection de $(b'c)$ et $(c'b)$, $(c'a)$ et $(a'c)$ et $(a'b)$ et $(b'a)$. Alors, α, β et γ sont alignés.

Démonstration. Faire une figure ! On envoie la droite $(\alpha\gamma)$ à l'infini. En d'autres termes, on étudie le même problème mais dans le plan affine $\mathcal{P}$ obtenu en retirant la droite $(\alpha\gamma)$. Mais

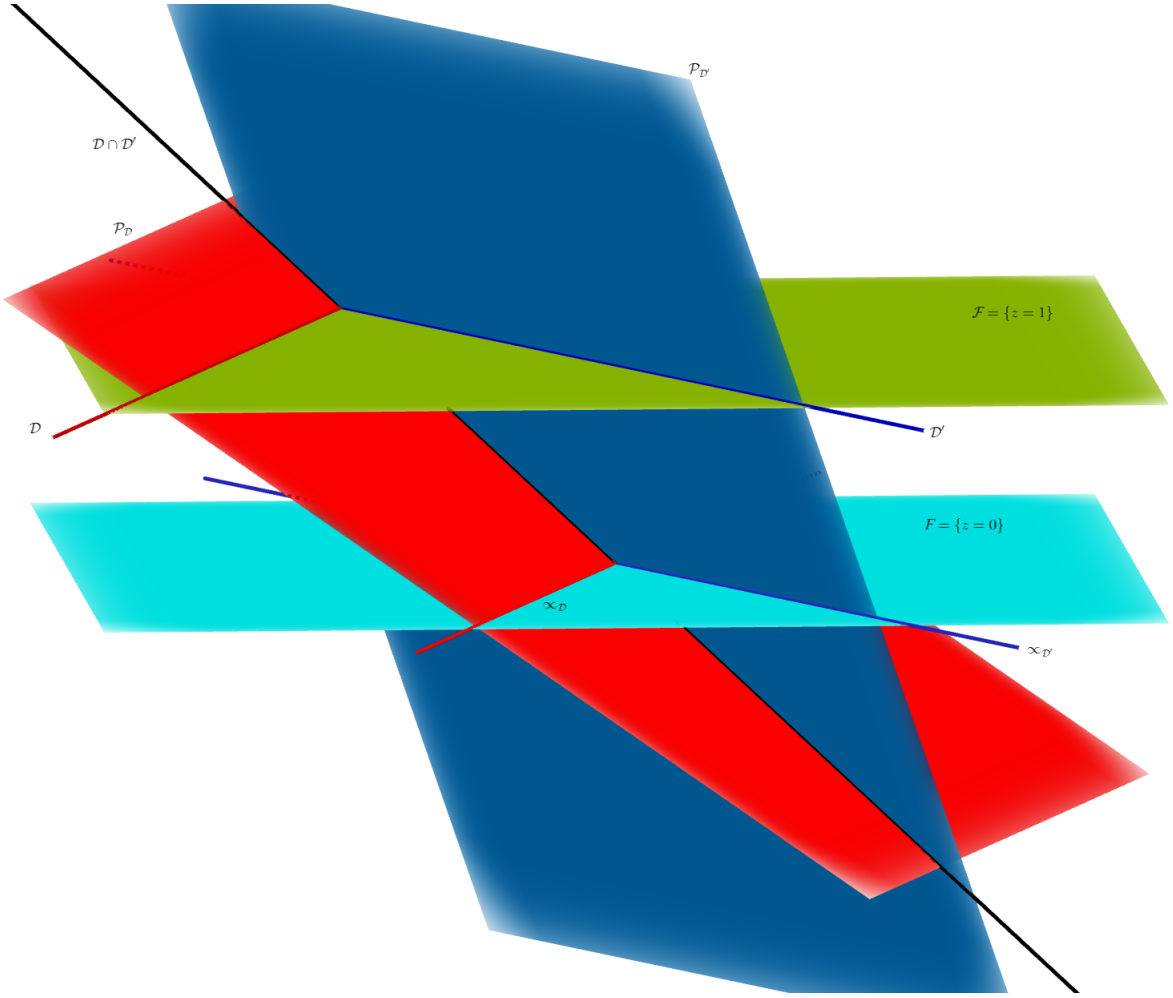

FIGURE 3.4 – Deux droites affines concourantes vue dans un plan projectif

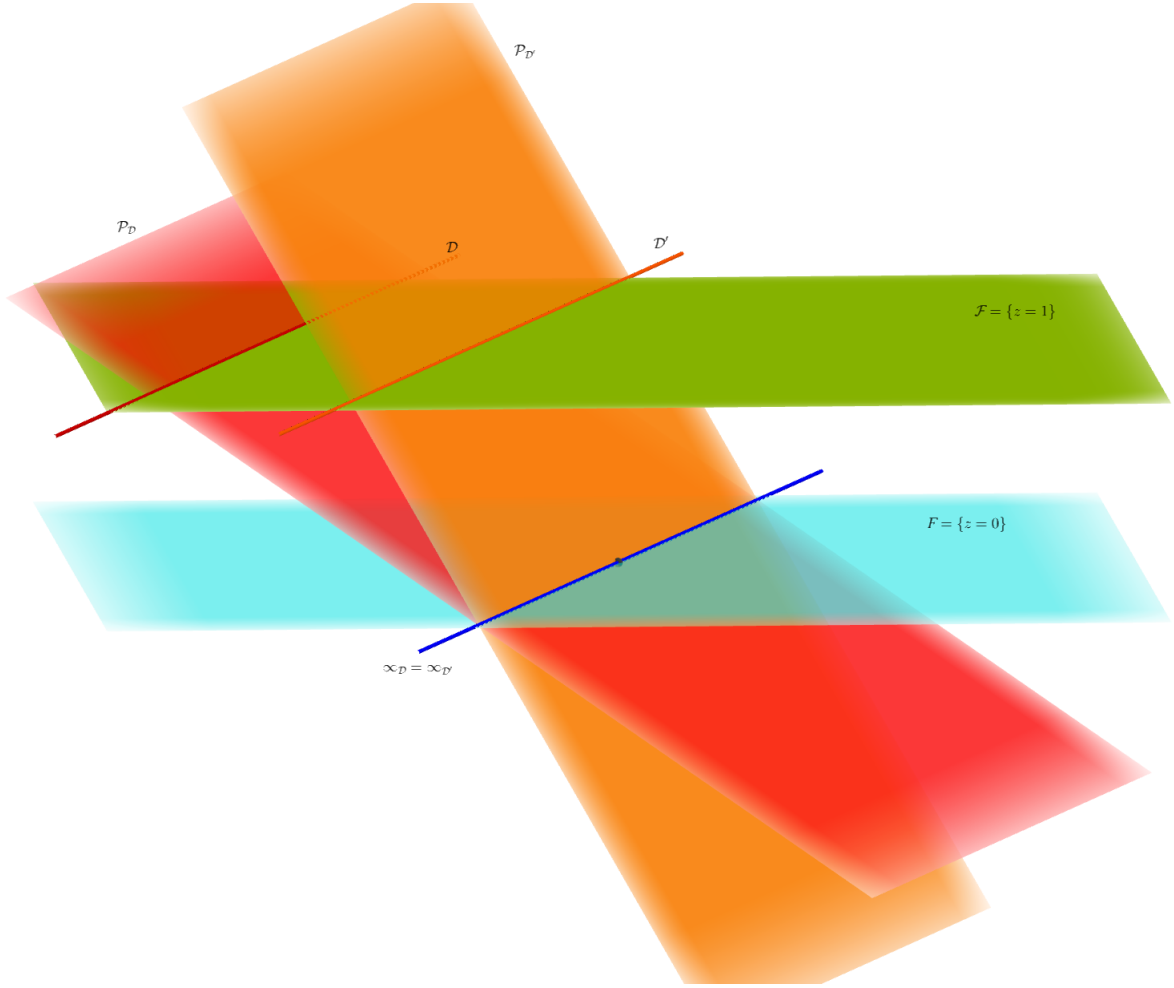

FIGURE 3.5 – Deux droites affines parallèles vue dans un plan projectif

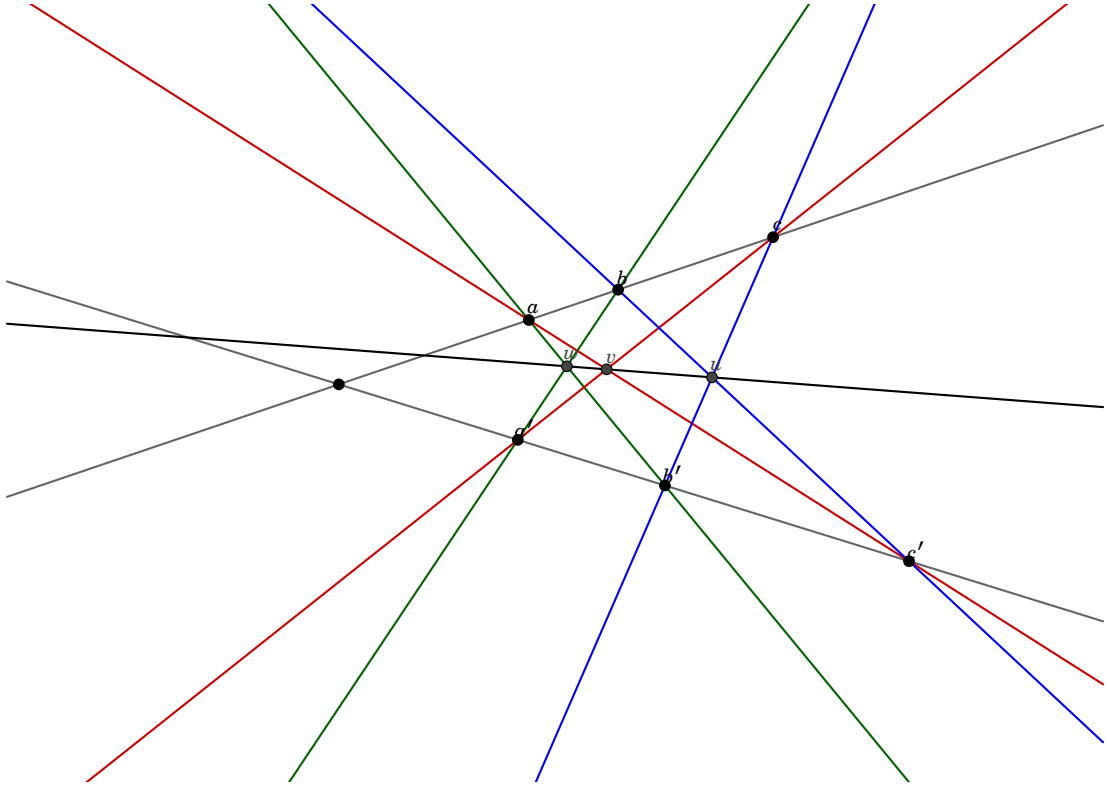

FIGURE 3.6 – Le Théorème de Pappus

dire α est à l'infini signifie que les droites $(b'c)$ et $(c'b)$ sont parallèles dans $\mathcal{P}$, de même pour γ et les droites $(a'b)$ et $(b'a)$. On refait une figure dans $\mathcal{P}$ cette fois ! *Cette opération s'appelle envoyer α et γ à l'infini.*

On souhaite montrer que β est sur la droite $(\alpha\gamma)$, c'est à dire à l'infini. Autrement dit, on veut montrer que les droites $(c'a)$ et $(a'c)$ sont parallèles.

Pour cela, on considère deux homothéties h et k de centre $D \cap D'$ tel que $h(c) = b$ et $k(b) = a$. L'hypothèse de parallélisme via le Théorème de Thalès montre que $h(b') = c'$ et $k(a') = b'$, ainsi $k \circ h(c) = a$ et $h \circ k(a') = c'$ mais $h \circ k = k \circ h$. Enfin, les homothéties envoient une droite sur une droite parallèle, d'où le résultat.

Si $D \cap D' \cap \mathcal{P} = \varnothing$ dans le plan affine $\mathcal{P}$. Autrement dit, si $D \cap D' \subset (\alpha\gamma)$ alors les droites affines D et D' sont parallèles. On considère alors des translations au lieu de considérer des homothéties. ■

R On voit apparaitre à la fin de la démonstration le fait important que deux homothéties de même centre commutent. Cet énoncé est équivalent au fait que le corps de base k est commutatif.

8. Le théorème de Desargues

Théorème III.2 — Théorème de Desargues, $\simeq 1620$. Soient abc et $a'b'c'$ deux triangles. Soient u, v, w les points d'intersection des droites bc et $b'c'$, ca et $c'a'$, ab et $a'b'$. Alors les points u, v, w sont alignés si et seulement si les droites aa', bb' et cc' sont concourantes.

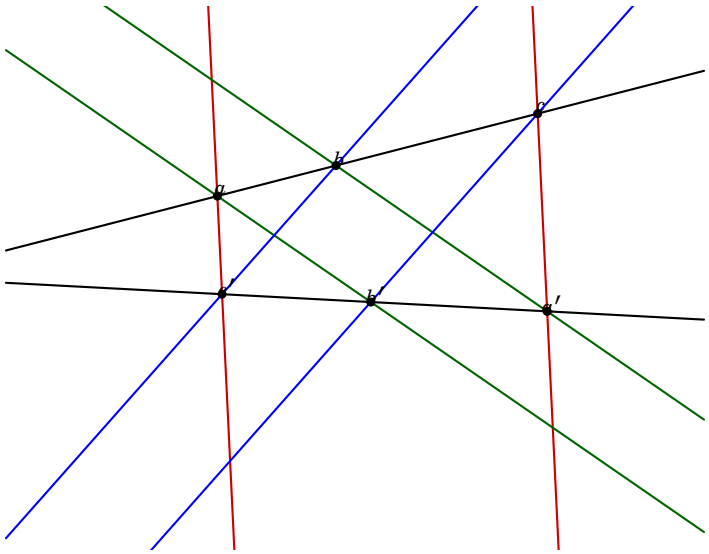

FIGURE 3.7 – Le Théorème de Pappus après envoi à l'infini

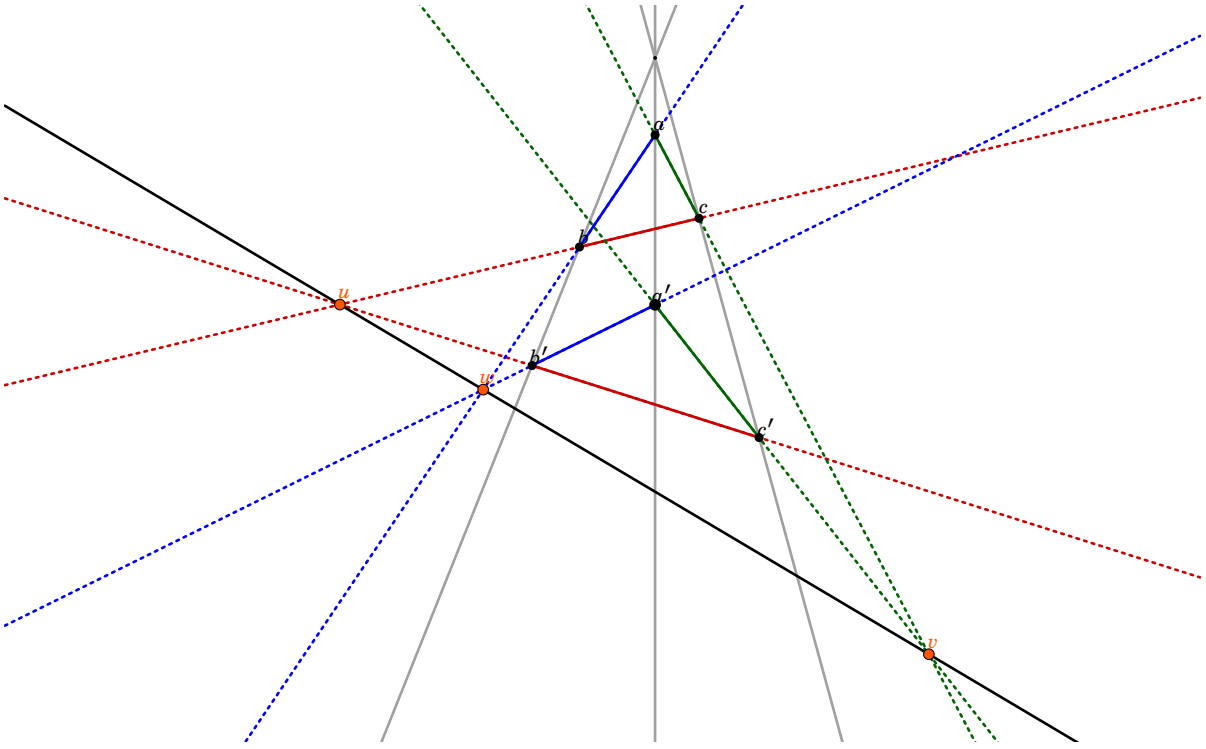

FIGURE 3.8 – Le Théorème de Desargues

Démonstration. Le sens direct sera démontré en TD. Le sens réciproque sera démontré par un argument très joli qui est l'objet de la prochaine section. ■

Fin du cours 7

IV Dualité projective

1. Dualité vectoriel

Si F est un sous-espace vectoriel de E alors *l'orthogonal* F° de F est défini par :

$$F^\circ = \{\varphi \in E^* \,|\, \varphi_{|F} = 0\} \leqslant E^*$$

C'est bien un sous-espace vectoriel et il est de dimension $\dim F^\circ = \dim E - \dim F$.

De même, si G est un sous-espace de E^*, on définit son *orthogonal* G° par :

$$G^\circ = \{x \in E \,|\, \forall \varphi \in G, \varphi(x) = 0\} \leqslant E$$

C'est bien un sous-espace vectoriel et il est de dimension $\dim G^\circ = \dim E - \dim G$.

On rappelle aussi que :

$$F^{\circ\circ} = F \quad \text{et} \quad F \subset G \Leftrightarrow G^\circ \subset F^\circ$$

que F, G soit un sous-espace vectoriel de E ou de E^*.

Un énoncé de géométrie projective est une assertion où les hypothèses portent sur des relations d'inclusion ou d'intersection entre des points, des droites, des plans, des coniques, etc... et les conclusions apportent de nouvelles informations sur d'autres inclusions ou intersections entre ses objets. Exemple : Les théorème de Pappus et Desargues.

Par conséquent, si on a un énoncé dans $\mathbb{P}(E)$, on peut le dualiser[2]. Pour cela, on commence par traduire les hypothèses dans $\mathbb{P}(E^*)$ puis on traduit les conclusions toujours dans $\mathbb{P}(E^*)$. Comme $\mathbb{P}(E^*)$ est un espace projectif comme les autres, c'est à dire isomorphe à $\mathbb{P}(E)$, on a obtenu un nouveau théorème !

2. La dualité : comment ca marche ?

On résume à présent tout cela lorsque $\dim E = 3$ (cas le plus intéressant pour nous).

$\mathbb{P}(E)$	E	E^*	$\mathbb{P}(E^*)$
$a \in \mathbb{P}(E)$ point	$a \subset E$ droite vectorielle	$a^\circ \subset E^*$ plan vectoriel	$\mathbb{P}(a^\circ) = A^\circ \subset \mathbb{P}(E^*)$ droite projective
$D = \mathbb{P}(P) \subset \mathbb{P}(E)$ droite projective	$P \subset E$ plan vectoriel	$P^\circ \subset E^*$ droite vectorielle	$d^\circ = \mathbb{P}(P^\circ) \in \mathbb{P}(E^*)$ point

Le point intéressant c'est que les inclusions, les alignements de 3 points ou de concourances de 3 droites se traduisent par dualité !

R On va éviter d'utiliser des $^\circ$ pour marquer la dualité, on a changé les minuscules en majuscules et inversement.

a, b, c points de $\mathbb{P}^2$	A, B, C droites duales de $\mathbb{P}^{2*}$
D droite de $\mathbb{P}^2$	d point dual de $\mathbb{P}^{2*}$
$a \in D$	$A \ni d$
$D =$ droite (ab)	$d =$ point $A \cap B$
a, b, c sont alignés sur D	A, B, C sont concourantes en d

2. si vous préférez le métamorphoser

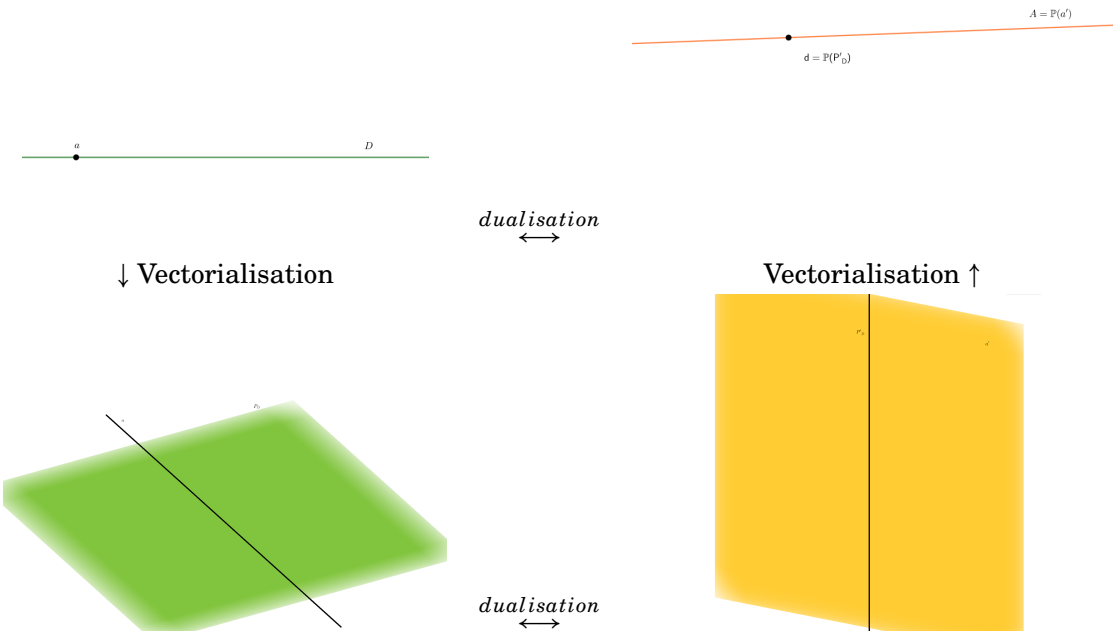

FIGURE 3.9 – Dualisation de l'assertion $a \in D$

R Les dernières lignes doivent se lire dans les deux sens, car le dual du dual est l'espace de départ.

Démonstration. Il suffit de regarder les figures suivantes :

■

3. Méthamorphose du Théorème de Pappus : le théorème de Brianchon

On commence par rappeler l'énoncé du théorème de Pappus.

Théorème IV.1 — Théorème de Pappus. Soient D, D' deux droites d'un plan projectif. Soient a, b, c trois points de D et a', b', c' trois points de D'. Soient u, v, w les points d'intersection de $(b'c)$ et $(c'b)$, $(c'a)$ et $(a'c)$ et $(a'b)$ et $(b'a)$. Alors, u, v et w sont alignés.

On applique la méthamorphose à Pappus, on obtient le théorème suivant :

Théorème IV.2 — Théorème de Brianchon (cas dégénéré). Soient d, d' deux points d'un plan projectif. Soient A, B, C trois droites concourantes en d et A', B', C' trois droites concourantes en d'. Soient U, V, W les droites joignant $B' \cap C$ et $C' \cap B$, $C' \cap A$ et $A' \cap C$ et $A' \cap B$ et $B' \cap A$. Alors, U, V, W sont concourantes.

4. Méthamorphose du sens direct du théorème de Desargues : sa réciproque

On rappelle l'énoncé du Théorème de Desargues dans le sens direct.

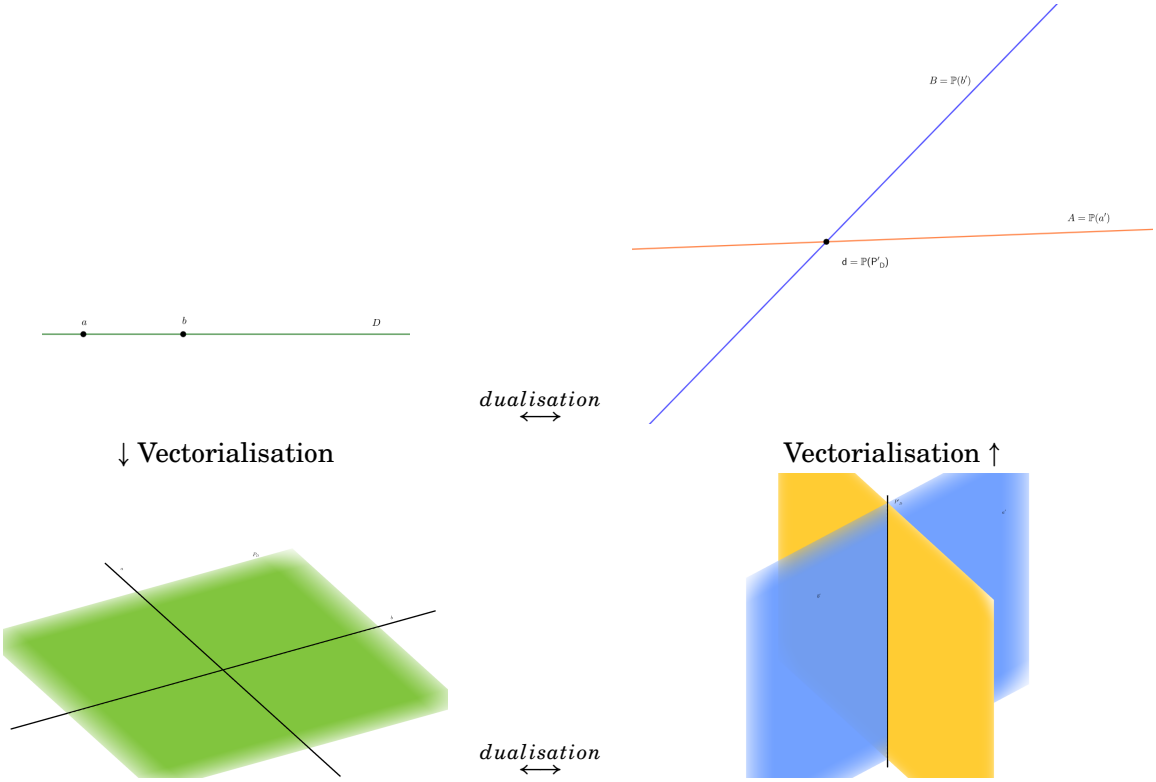

FIGURE 3.10 – Dualisation de l'assertion $D = (ab)$ (ou de $A \cap B = d$)

Théorème IV.3 — Théorème de Desargues, sens direct. Soient abc et $a'b'c'$ deux triangles. Soient u,v,w les points d'intersection des droites bc et $b'c'$, ca et $c'a'$, ab et $a'b'$. Si les points u,v,w sont alignés alors les droites aa', bb' et cc' sont concourantes.

On applique la méthamorphose à Desargues sens direct, on obtient le théorème suivant :

Théorème IV.4 — Théorème de Desargues, réciproque. Soient A,B,C trois droites et A',B',C' trois droites. Soient U,V,W les droites passant par $B \cap C$ et $B' \cap C'$, $C \cap A$ et $C' \cap A'$, $A \cap B$ et $A' \cap B'$. Si les droites U,V,W sont concourantes alors les points $A \cap A'$, $B \cap B'$ et $C \cap C'$ sont alignés.

R Faire une figure de l'énoncé précédent, on s'aperçoit qu'il s'agit de la réciproque du sens direct du Théorème de Desargues. pour cela, il faut commencer par s'apercevoir que cette fois-ci, on a une hypothèse de concourance et une conclusion d'alignement. Ensuite, il faut bien regarder la figure et et renommer les choses suivantes :

- $A \cap B \rightsquigarrow c$, etc...
- $U \rightsquigarrow (aa')$
- $A \cap A' \rightsquigarrow u$

On réécrit l'énoncé du dual de Desargues après avec ce changement de notation. Soient U,V,W les droites passant par a et a', b et b', c et c'. Si les droites U,V,W sont concourantes alors les points $(bc) \cap (b'c')$, $(ac) \cap (a'c')$ et $(ab) \cap (a'b')$ sont alignés.

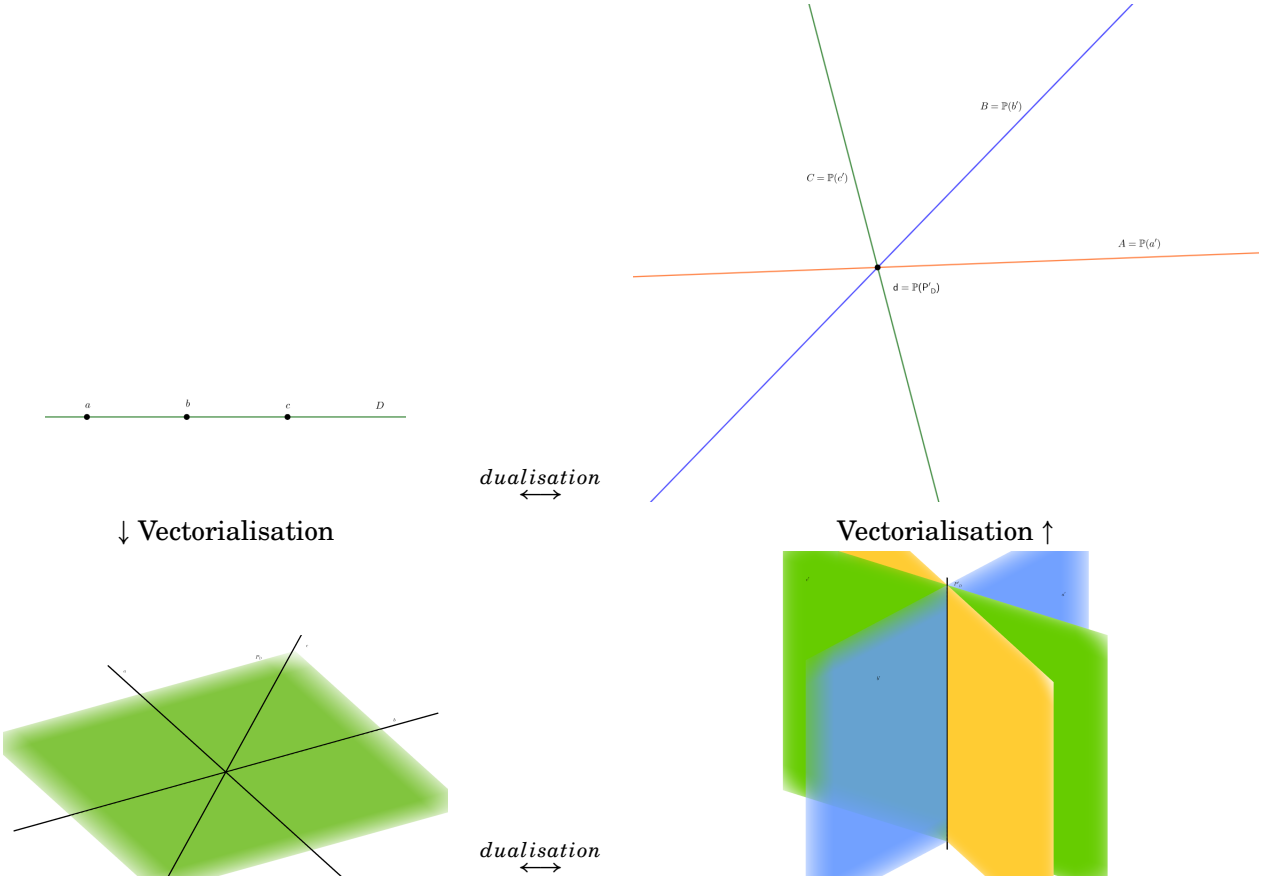

FIGURE 3.11 – Dualisation de l'assertion a, b, c sont alignés (ou de A, B, C sont concourantes)

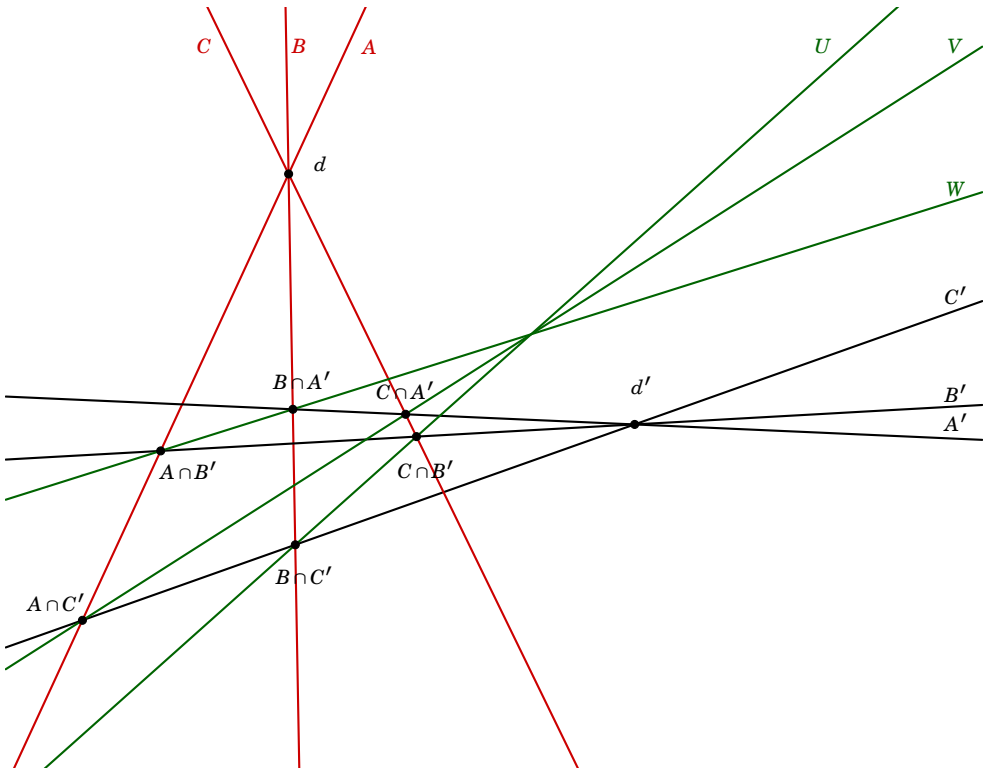

FIGURE 3.12 – Le Théorème de Brianchon

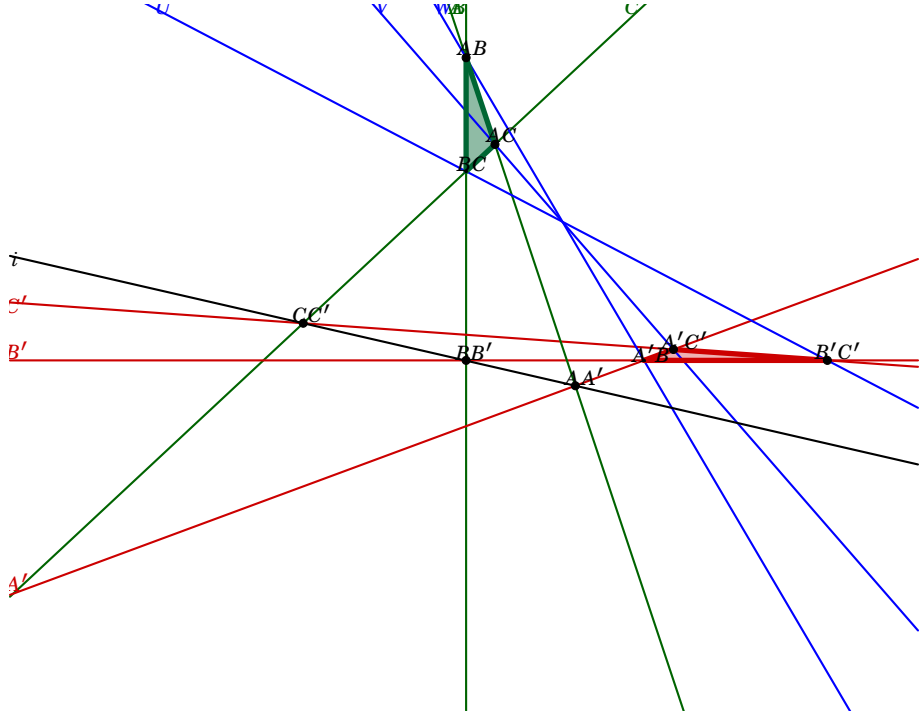

FIGURE 3.13 – La méthamorphose du sens direct du Théorème de Desargues

V Homographies

1. Transformations projectives et le groupe projectif

Soient E, E' deux espaces vectoriels et $f : E \to E'$ une application linéaire, si D est une droite de E tel que $D \cap \ker(f) = \{0\}$ alors $f(D)$ est une droite de E'. Ainsi, f induit une *application projective* : $\mathbb{P}(f) : \mathbb{P}(E) \setminus \mathbb{P}(\ker(f)) \to \mathbb{P}(E')$ qui vérifie $\pi' \circ f = \mathbb{P}(f) \circ \pi$. En d'autres termes, le diagrame suivant :

$$\begin{array}{ccc} E & \xrightarrow{f} & E' \\ \pi \downarrow & & \downarrow \pi \\ \mathbb{P}(E) & \xrightarrow{\mathbb{P}(f)} & \mathbb{P}(E') \end{array}$$

est commutatif.

Presque toujours, on se limite au cas où f est un isomorphisme. Dans ce cas, on dit que $\mathbb{P}(f)$ est une *homographie*.

Exercice 3.4 Vérifier pour tout couple d'isomorphismes $f, g : E \to E$, on a $\mathbb{P}(f \circ g) = \mathbb{P}(f) \circ \mathbb{P}(g)$ et $\mathbb{P}(f)$ est une bijection et que son inverse est $\mathbb{P}(f^{-1})$. ∎

On note $\mathrm{PGL}(E)$ le *groupe des homographies* de $\mathbb{P}(E)$.

Proposition V.1 L'application $\mathbb{P} : \mathrm{GL}(E) \to \mathrm{PGL}(E)$ est un morphisme surjectif de noyau le groupe des homothéties de E.

Démonstration. Il nous reste à vérifier que le noyau de $\mathbb{P}$ est le groupe des homothéties. Un élément du noyau est une application linéaire $f : E \to E$ qui vérifie pour toute droite D de E, on a $f(D) = D$.

On a donc pour tout $u \neq 0$, qu'il existe un scalaire $\lambda_u \in k$ tel que $f(u) = \lambda_u u$. Il faut montrer que λ_u est indépendant de u. Soient u, v non colinéaires, on a :

$$f(u) = \lambda_u u \quad f(v) = \lambda_v v \quad f(u+v) = \lambda_{u+v} u + \lambda_{u+v} v = \lambda_u u + \lambda_v v$$

On conlut aisément. ■

R Le groupe Z des homothéties de $\mathrm{GL}(E)$ est aussi le centre de $\mathrm{GL}(E)$. Enfin, $Z \simeq k^*$

2. Coordonnées homogènes

Soit $(e_1, \ldots, e_{n+1})$ une base de l'espace vectoriel E. Un point $m \in \mathbb{P}(E)$ peut-être décrit par les coordonnées du vecteur qui engendre la droite m. Deux $(n+1)$-uplets $(x_1, \ldots, x_{n+1})$ et $(x'_1, \ldots, x'_{n+1})$ représentent le même point m si et seulement s'il existe un scalaire non nul λ tel que :

$$x_i = \lambda x'_i, \quad \text{pour tout } i$$

On appelle la classe d'équivalence de $(x_1, \ldots, x_{n+1})$ des *coordonnées homogènes* pour m, on la note :

$$[x_1 : \ldots : x_{n+1}]$$

R repères projectifs, on ne fait pas ...

3. Homographies de la droite

Lien $k\mathbb{P}^1 \simeq k \cup \{\infty\}$

Soit E un espace vectoriel de dimension 2. Soit (e_1, e_2) une base de E. On rappelle que ce choix induit une bijection canonique $\varphi : k\mathbb{P}^1 \to k \cup \{\infty\}$ que nous allons à présent écrire à l'aide des coordonnées homogènes :

$$\begin{array}{rccccc} \varphi : & k\mathbb{P}^1 & \to & k \cup \{\infty\} & & \\ & [x:y] & \mapsto & x/y & \text{si} & y \neq 0 \\ & [1:0] & \mapsto & \infty & & \end{array}$$

Homographies de la droite projective écrites dans $k \cup \{\infty\}$

On va à présent, écrire les homographies de $\mathbb{P}(E)$ dans $k \cup \{\infty\}$. Une homographie de la droite projective vient d'un isomorphisme $f : E \to E$ d'un plan vectoriel. Dans la base (e_1, e_2) la matrice de f est $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où $ad - bc \neq 0$. Ce qui signifie que $f(x,y) = (ax + by, cx + dy)$. Supposons $y \neq 0$ et Écrivons $z = x/y$, ainsi $(x,y) \sim (z,1)$, alors

$$f(z,1) = (az + b, cz + d) \sim \left(\frac{az+b}{cz+d}, 1 \right)$$

pourvu que $cz + d \neq 0$.

On adopte la notation suivante, on note l'homographie induite par f :

$$f : k \cup \{\infty\} = k\mathbb{P}^1 \circlearrowleft, \qquad z \mapsto \frac{az+b}{cz+d}$$

en sous-entendant la convention suivante :

$$f(\infty) = f([1:0]) = a/c \qquad f(-d/c) = \infty$$

On sous-entend aussi les règles suivantes, pour $\lambda \neq 0$:

$$\lambda/0 = \infty \quad 0/\lambda = 0$$

Le point clé étant que la situation $0/0$ n'arrive jamais car $ad - bc \neq 0$.

Démonstration. Commençons par voir qu'il n'y a pas vraiment de souci à se faire dans les cas litigieux.

- Si $y = 0$ alors $f(1,0) = (a,c)$
  - ◇ si $c \neq 0$ alors $(a,c) \sim (a/c, 1)$
  - ◇ si $c = 0$ alors $(a,c) \sim (1,0)$ car dans ce dernier cas $a \neq 0$ puisque $ad - bc \neq 0$.
- Si $cz + d = 0$, on a deux cas :
  - ◇ Si $c \neq 0$ alors $z = -d/c$ et $f(z,1) = ((-ad + bc)/c, 0) \sim (1,0) = \infty$ car $ad - bc \neq 0$.
  - ◇ Si $c = 0$ alors $d = 0$, ce cas n'est pas possible, en fait...

■

R Vous pouvez vérifier que ces notations sont particulièrement adaptés au cas où la droite projective est construite comme le complété projectif de la droite affine.

4. Choix de l'infini (suite)

Revenons à la question de l'expédition d'objets à l'infini. Une autre façon de voir les choses est de dire qu'on applique une homographie à une figure pour la transformer en une nouvelle figure plus simple à analyser. Très bien dit dans Audin.

Fin du cours 8

5. Homographies et transformation affines

Proposition V.2 Soient $\mathcal{F}$ un espace affine dirigée par un espace vectoriel F et $\mathbb{P}(F \oplus k) = \mathcal{F} \sqcup \mathbb{P}(F)$ son complété projectif.

- Toute homographie g qui préserve l'hyperplan à l'infini $\mathbb{P}(F)$ définit une transformation affine φ de $\mathcal{F}$.
- Inversement, toute transformation affine φ de $\mathcal{F}$ se prolonge de façon unique en une homographie g de $\mathbb{P}(F \oplus k)$ qui préserve l'hyperplan à l'infini.

De plus, dans ce cas, on a :

$$\mathbb{P}(\overrightarrow{\varphi}) = g_{|\mathbb{P}(H)}$$

Enfin, si f est l'unique automorphisme de $F \oplus k$ tel que $\mathbb{P}(f) = g$ et $f(F \times \{1\}) = F \times \{1\}$ alors :

$$\overrightarrow{\varphi} = f_{|H}$$

Démonstration. Soit $g : \mathbb{P}(F \oplus k) \to \mathbb{P}(F \oplus k)$ une homographie qui préserve l'hyperplan à l'infini $\mathbb{P}(F)$. Ainsi, g préserve le complémentaire $\mathcal{F} = \mathbb{P}(F \oplus k) \setminus \mathbb{P}(F)$. On veut montrer que l'application g restreinte à $\mathcal{F}$ est affine.

On note f un automorphisme linéaire $F \oplus k$ qui induit g, on a :

$$f(u,0) = (h(u),0) \qquad \text{et} \qquad f(0,1) = (v,a)$$

où h est un automorphisme linéaire de F, v un vecteur de F et a un scalaire non-nul. Pour ceux qui préfèrent les matrices, on est en train de dire que dans une base adaptée à la décomposition $F \oplus k$, la matrice de f est de la forme :

$$\begin{pmatrix} h & v \\ 0 & a \end{pmatrix}$$

On peut choisir f de tel façon que $a = 1$. Autrement dit, dans la classe de g, il existe un représentant qui vérifie $a = 1$. Il s'agit de l'unique représentant f de g qui vérifie $f(F \times \{1\}) = F \times \{1\}$.

Ainsi, l'hyperplan affine $\mathcal{F} = F \times \{1\}$ est préservé par f. Comme l'application f est linéaire, l'application φ induite sur $\mathcal{F}$ est donc affine.

En effet, fixons le point $(0,1)$ comme origine de $\mathcal{F}$. Pour tout point $M = (u,1) \in \mathcal{F}$, on a :

$$\overrightarrow{g(O)g(M)} = f(u,1) - f(0,1) = (h(u)+v,1) - (v,1) = (h(u),0)$$

Ainsi, $\varphi = g_{|\mathcal{F}}$ est affine de linéarisé h.

Respirons deux minutes, avant de montrer la réciproque, en réalisant que l'on a montré le "de plus" et le "enfin". On vient voir que :

$$\overrightarrow{\varphi} = h = f_{|H}$$

Ce qui montre le "enfin". Ensuite, le "enfin" implique le "de plus", puisque deux automorphismes f, f' qui induisent une même homographie sont multiples l'un de l'autre.

Inversement, soit $\varphi : \mathcal{F} \to \mathcal{F}$ une application affine. On identifie $\mathcal{F}$ avec l'hyperplan de hauteur 1 de l'espace vectoriel $F \oplus k$. On note h sa partie linéaire et on pose $\varphi(0,1) =: (v,1)$. On définit :

$$\begin{array}{rccc} f : & F \oplus k & \to & F \oplus k \\ & (u,\lambda) & \mapsto & \lambda\varphi(0,1) + (h(u),0) = (h(u) + \lambda v, \lambda) \end{array}$$

Ainsi, f est linéaire préserve $\mathcal{F}$, l'application induite sur $\mathcal{F}$ est φ. L'homographie induite par f possède donc les propriétés attendues.

Montrons à présent l'unicité. On va utiliser le "de plus" de la première partie de la démonstration. Soit g une homographie de $F \oplus k$ qui préserve $\mathcal{F}$ et induit φ sur $\mathcal{F}$. On a bien sûr $g = \varphi$ sur $\mathcal{F}$, et par le "de plus" de la première partie, on a que :

$$g_{|\mathbb{P}(H)} = \mathbb{P}(\overrightarrow{\varphi})$$

L'homographie g est donc déterminé par φ. ■

Cette démonstration permet d'identifier le groupe affine avec un sous-groupe du groupe linéaire ou du sous-groupe projectif linéaire.

Proposition V.3 On a :

$$\mathrm{GA}(k^d) = \left\{ \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \,\middle|\, A \in \mathrm{GL}_d(k), b \in k^d \right\} \leqslant (\mathrm{P})\mathrm{GL}_{d+1}(k)$$

6. Action $\mathrm{PSL}(E) \curvearrowright \mathbb{P}(E)$

Le *groupe spécial linéaire* $\mathrm{SL}(E)$ est le sous-groupe des automorphismes linéaires de E de déterminant 1. Le sous-groupe $Z \cap \mathrm{SL}(E)$ est distingué dans $\mathrm{SL}(E)$, où Z est le groupe des homothéties. Le quotient $\mathrm{PSL}(E) = \mathrm{SL}(E)/Z \cap \mathrm{SL}(E)$ s'appelle le groupe *projectif spécial linéaire*. On peut montrer que $Z \cap \mathrm{SL}(E)$ est le centre de $\mathrm{SL}(E)$. L'action de $\mathrm{PSL}(E) \curvearrowright \mathbb{P}(E)$ est fidèle.

Proposition V.4 $\mathrm{PSL}(E) \curvearrowright \mathbb{P}(E)$ est 2-transitive.

Démonstration. On peut supposer que $E = k^{n+1}$. Soient m, m' deux points de $k\mathbb{P}^n$ distincts. Soient u, u' deux vecteurs non nuls des droites m, m' respectivement. Les vecteurs u, u' ne sont pas colinéaires. On complète la famille (u, u') en une base $(u_1, u_2, \ldots, u_{n+1})$ de E.

Pour tout $\lambda \in k$, on a :

$$\det(\lambda u_1, u_2, \ldots, u_{n+1}) = \lambda \det(u_1, u_2, \ldots, u_{n+1})$$

On peut donc supposer que la base $(u_1, u_2, \ldots, u_{n+1})$ est de déterminant 1, que u_1 engendre m et u_2 engendre m'. Ainsi, si on note g la matrice des $(u_1, u_2, \ldots, u_{n+1})$, on a $g(e_1) = u_1$, $g(e_2) = u_2$. Ce qui montre la 2-transitivité. ■

Proposition V.5 Si $\dim E = 2$ alors $\mathrm{PGL}(E) \curvearrowright \mathbb{P}(E)$ est simplement 3-transitive.

Démonstration. Grâce à la proposition précédente, il suffit de montrer que le stabilisateur de 0 et ∞ agit simplement transitivement sur k^* mais le stabilisateur de 0 et ∞ est le groupe des matrices de la forme :

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

qui s'identifie à k^* et l'action de $\mathrm{Stab}_{0,\infty}$ sur $k^* \subset k \cup \{\infty\}$ s'identifie à l'action par translation de k^* sur lui-même, elle est donc simplement transitive. ■

VI Birapport

En géométrie euclicienne, la distance entre deux points est essentiel. En géométrie affine, les rapports de "distance" entre deux points sont essentiels. En géométrie projective, les rapports de rapport de distance entre 4 points seront essentiels, on les appelle les birapports !

1. C'est quoi ?

On commence par appliquer la dernière proposition : Si $\dim E = 2$ alors $\mathrm{PGL}(E) \curvearrowright \mathbb{P}(E)$ est simplement 3-transitive. Elle nous dit que si a,b,c sont trois points distincts de $k\mathbb{P}^1 = k \cup \{\infty\}$ alors il existe une unique homographie g tel que :

$$g(a) = \infty \qquad g(b) = 0 \qquad g(c) = 1$$

Définition VI.1 Soient a,b,c trois points distincts d'une droite projective. Soit d un autre point. Il existe une unique homographie $g : D \to k \cup \{\infty\}$ tel que $g(a) = \infty$, $g(b) = 0$ et $g(c) = 1$. On appelle *birapport* de (a,b,c,d), l'élément $g(d) \in k \cup \{\infty\}$, on le note $[a,b,c,d]$.

R Par définition, on a :
- $[a,b,c,a] = \infty$
- $[a,b,c,b] = 0$
- $[a,b,c,c] = 1$

Comme l'homographie g est une bijection. Le birapport $[a,b,c,d] \in k \setminus \{0,1\}$ si et seulement si a,b,c,d sont distincts. De plus, pour tout triplet (a,b,c) de points distincts, pour tout $x \in k \cup \{\infty\}$, il existe un unique point d tel que $[a,b,c,d] = x$, tout simplement, $d := g^{-1}(x)$.

Démonstration. Soit φ un isomorphisme $\varphi : \overline{D} \to k^2$, il existe une unique homographie $f : \mathbb{P}^1(k) \to \mathbb{P}^1(k)$ tel que :

$$f(\varphi(a)) = \infty \quad f(\varphi(b)) = 0 \quad f(\varphi(c)) = 1$$

Il existe donc une homographie $g : \mathbb{P}(E) \to \mathbb{P}^1(k)$ tel que :

$$g(a) = \infty \quad g(b) = 0 \quad g(c) = 1$$

Il suffit de prendre $g = f \circ \varphi$. Montrons, à présent que g est unique. Soit g' une homographie telle que :

$$g'(a) = \infty \quad g'(b) = 0 \quad g'(c) = 1$$

Ainsi, l'homographie $g' \circ g^{-1} : \mathbb{P}^1(k) \to \mathbb{P}^1(k)$ fixe les points $\infty, 0$ et 1. La proposition V.5 montre que $g' \circ g^{-1} = \mathrm{Id}$, par suite, $g = g'$. D'où, l'unicité. ∎

Proposition VI.1 — Conservation du birapport. Soient D, D' deux droites projectives. Soient $a_1,a_2,a_3,a_4 \in D$ et $a'_1,a'_2,a'_3,a'_4 \in D'$ tels que les 3 premiers points de chaque quadruplet sont distincts. Pour qu'il existe une homographie $f : D \to D'$ telle que $f(a_i) = a'_i$, il faut et il suffit que :

$$[a_1,a_2,a_3,a_4] = [a'_1,a'_2,a'_3,a'_4]$$

En particulier, si $f : D \to D'$ est une homographie alors :

$$\forall a_1,a_2,a_3,a_4 \in D, \quad \text{avec } \sharp\{a_1,a_2,a_3\} = 3, \quad [f(a_1),f(a_2),f(a_3),f(a_4)] = [a_1,a_2,a_3,a_4]$$

Démonstration. Supposons qu'il existe une telle homographie f. On note g' l'unique homographie $g' : D \to k \cup \{\infty\}$ tel que $g'(a'_1) = \infty$, $g'(a'_2) = 0$ et $g'(a'_3) = 1$. Par définition du birraport, on a :

$$[a'_1,a'_2,a'_3,a'_4] = g'(a'_4)$$

Mais $g' \circ f$ est l'unique homographie qui envoie a_1 sur ∞, a_2 sur 0 et a_3 sur 1. Par conséquent :

$$[a_1,a_2,a_3,a_4] = g' \circ f(a_4) = g'(a'_4) = [a'_1,a'_2,a'_3,a'_4]$$

Ainsi, le birapport est conservé par les homographies.

Inversement, supposons que $[a_1,a_2,a_3,a_4] = [a'_1,a'_2,a'_3,a'_4]$, on note g, respectivement g', l'unique homographie telle que :

$$g(a_1) = \infty, \quad g(a_2) = 0, \quad g(a_3) = 1 \quad \text{et} \quad g'(a'_1) = \infty, \quad g'(a'_2) = 0, \quad g'(a'_3) = 1$$

et on pose $f = g'^{-1} \circ g$. On doit vérifier que $f(a_4) = a'_4$. On a :

$$f(a_4) = g'^{-1} \circ g(a_4) = g'^{-1}([a_1,a_2,a_3,a_4]) = g'^{-1}([a'_1,a'_2,a'_3,a'_4]) = a'_4$$

■

R On peut donc parler de birapport de 4 points alignés (avec les 3 premiers distincts) dans un espace projectif quelconque.

2. Calcul du birapport

Proposition VI.2 Soient $a,b,c,d \in k \cup \{\infty\}$. Les trois premiers étant supposés distincts. Alors :

$$[a,b,c,d] = \frac{d-b}{d-a} \Big/ \frac{c-b}{c-a} = \frac{(d-b)(c-a)}{(d-a)(c-b)}$$

Démonstration. On commence par supposer $a,b,c \in k$. L'unique homographie qui envoie a sur ∞, b sur 0 et c sur 1 est donnée par :

$$z \mapsto \frac{(z-b)(c-a)}{(z-a)(c-b)}$$

puisqu'elle a un pôle en a, un zéro en b. Le birapport est par définition l'image par cette homographie de d... Remarquer que si $d = \infty$, la formule donne $[a,b,c,d] = \frac{c-a}{c-b}$.

Si $a = \infty$ alors l'égalité annoncé devient :

$$[a,b,c,d] = \frac{(d-b)}{(c-b)}$$

On reprend la stratégie précédente, l'unique homographie envoie ∞ sur ∞, b sur 0 et c sur 1 est donnée par :

$$z \mapsto \frac{z-b}{c-b}$$

Le birapport est par définition l'image par cette homographie de d... Remarquer que si $d = \infty$, la formule donne $[a,b,c,d] = \infty$. On laisse les deux cas restants au lecteur. ■

R Soient a,b deux points distincts d'une droite affine. Il existe une unique application ... Je sais pas si je dis ou pas...

R Soient a,b,c trois points distincts d'une droite affine. On a :

$$[a,b,c,\infty] = \frac{c-a}{c-b} = \frac{\overline{ca}}{\overline{cb}}$$

On retrouve le rapport de longueur de la géométrie affine.

Proposition VI.3 Si a,b,c,d sont 4 points alignés distincts alors on a les formules suivantes :

$$[a,b,c,d] = [b,a,c,d]^{-1} = [a,b,d,c]^{-1}$$

$$[a,b,c,d] + [a,c,b,d] = 1$$

Démonstration. Voir feuille de TD. ■

R Étant donnés quatre points a,b,c,d distincts d'une droite projective, on peut les arranger de 24 façons différentes. Cependant, le birapport de ces quatres points ne prendra (au +) que 6 valeurs. En effet si $[a,b,c,d] = \lambda$ alors les 6 valeurs possibles pour les birapports $[\sigma(a),\sigma(b),\sigma(c),\sigma(d)]$ sont :

$$\lambda, \quad \frac{1}{\lambda}, \quad 1-\lambda, \quad 1-\frac{1}{\lambda}, \quad \frac{1}{1-\lambda}, \quad \frac{\lambda}{\lambda-1}$$

3. Birapport de 4 droites concourantes

Proposition VI.4 — Définition d'une perspective. Soit D,D' deux droites d'un plan projectif. Soit o à l'extérieur de D,D', l'application $D \to D'$ donnée par $x \mapsto (ox) \cap D'$ qui est bien définie, est une homographie. On appelle une telle application une *perspective*.

Lemma VI.5 L'application $\varphi_{o,D'} : \mathbb{P}^2 \setminus o \to D'$ donnée par $m \mapsto m' := (om) \cap D'$ est induite par l'application linéaire : projection sur $\overline{D'}$ parallèlement à o.

On rappelle que si X est un sous-espace projectif de $\mathbb{P}(E)$ alors $\overline{X}$ est l'unique sous-espace vectoriel de E tel que $\mathbb{P}(\overline{X}) = X$.

Démonstration. Ne pas oublier qu'un point de l'espace projectif $\mathbb{P}(E)$ est une droite vectorielle de E. En projectif, le point m' est caractérisé par les deux assertions suivantes :

$$(om) = (om') \quad \text{et} \quad m' \in D'$$

En vectoriel, la droite vectorielle m' est caractérisée par le fait que :

$$o + m = o + m' \quad \text{et} \quad m' \subset \overline{D'}$$

Soit x un vecteur non-nul de la droite m, on a $E = o \oplus \overline{D'}$, donc on peut écrire $x = u + v$ avec $u \in \overline{D'}$ et $v \in o$. On a donc :

$$o + m = \mathrm{Vect}(o,u) \quad \text{et} \quad u \in \overline{D'}$$

Donc $m' = \mathrm{Vect}(u)$. ■

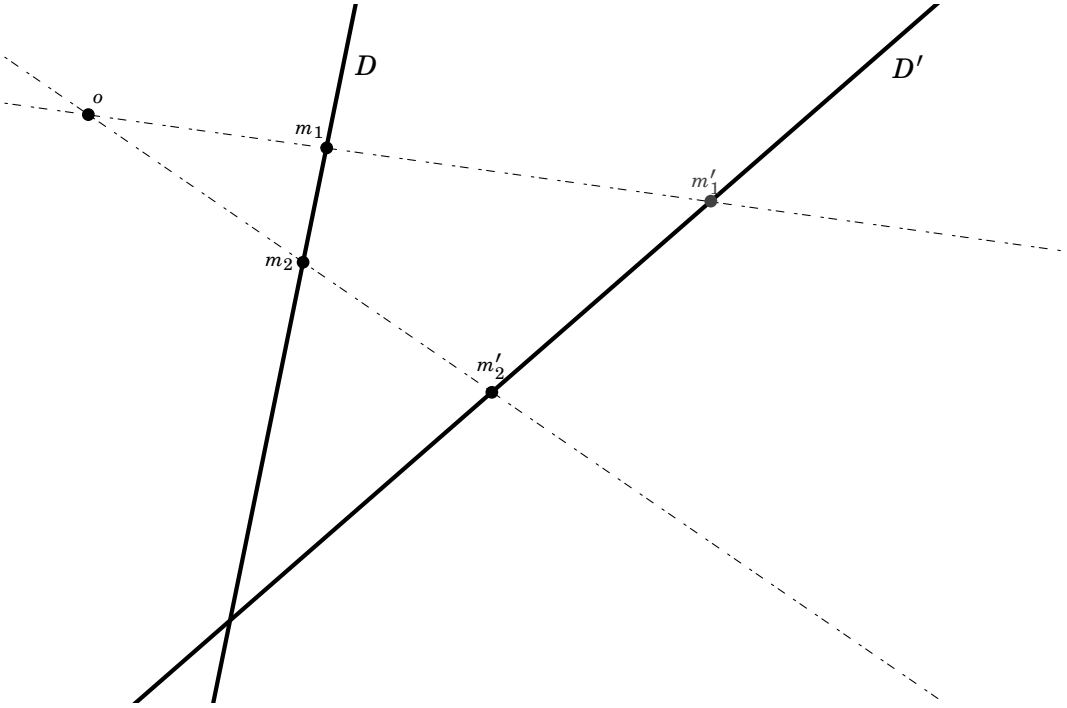

FIGURE 3.14 – Définition d'une perspective $m \mapsto m'$.

Démonstration. L'application annoncée est simplement la restriction de $\varphi_{o,D'}$ à la droite D. Cette dernière est une homographie puisque $p_{o,\overline{D'}|\overline{D}} : \overline{D} \to \overline{D'}$ est un isomorphisme puisque son noyau est $o \cap \overline{D}$. ■

Corollaire VI.6 — Définition du birapport de 4 droites. Soient $\ell_1, \ell_2, \ell_3, \ell_4$ 4 droites d'un plan projectif **concourantes en un point** z telles que les 3 premières sont distinctes. Si D, D' sont deux droites ne passant par z alors :

$$[x_1, x_2, x_3, x_4] = [x'_1, x'_2, x'_3, x'_4]$$

où $x_i = \ell_i \cap D$ et $x'_i = \ell_i \cap D'$. Ce nombre est le birapport des 4 droites $\ell_1, \ell_2, \ell_3, \ell_4$, notées $[\ell_1, \ell_2, \ell_3, \ell_4]$.

Fin du cours 9

4. Division harmonique

C'est quoi ?

Définition VI.2 On dit que 4 points alignés forment une division harmonique lorsque leur birapport est égale à -1.

R Si a,b,c sont trois points d'une droite affine alors les points a,b,c,∞ forment une division harmonique si et seulement si c est le milieu de $[a,b]$. *On remarquera qu'"être le milieu" est une notion affine pas une notion euclidienne*. Tout simplement car $[a,b,c,\infty] = \frac{ca}{cb} = -1$.

R Si (a,b,c,d) est un quadruplet harmonique alors (b,a,c,d) et (a,b,d,c) sont aussi des quadruplets harmoniques.

Construction du 4ème harmonique dans $k\mathbb{P}^2$

Proposition VI.7 Soient a,b,c trois points alignés sur une droite d'un plan projectif. La construction indiquée dans la figure 3.15 construit l'unique point d tel que (a,b,c,d) est un quadruplet harmonique.

R Durant la construction, il y a trois choix un point m extérieur à (ab), deux points p,q sur (mc) distincts et distincts de m et c. La conclusion montre que le point d ne dépend pas de ces choix. Essayer sur Geogebra !

Démonstration. Il faut et il suffit de vérifier que $[a:b:c:d] = -1$. On envoie (mc) à l'infini. On obtient la figure de droite de la figure 3.15. Le quadrilatère $qprs$ de la construction devient un parallélogramme. La droite (md) devient la droite parallèle aux côtés pq et rs de ce parallélogramme passant par l'intersection des diagonales de celui-ci. Ainsi, $(md)\cap(ps)$ est le milieu de $[ps]$ et $(md)\cap(qr)$ est le milieu de $[qr]$. Le quadrilatère $bqra$ est aussi un parallélogramme. La droite (md) est parallèle aux côtés bq et ra de ce parallélogramme, par suite d est le milieu de $[ab]$. ∎

VII Le théorème fondamental de la géometrie projective

Définition VII.1 Une *collinéation* d'un espace projectif $k\mathbb{P}^d$ est une bijection $\varphi : k\mathbb{P}^d \circlearrowleft$ qui préserve l'ensemble des droites projectives.

Définition VII.2 Une application $u : E \to E$ est dite *semi-linéaire* lorsqu'il existe un automorphisme σ du corps k tel que :

- $\forall x,y \in E,\ u(x+y) = u(x)+u(y)$.
- $\forall x \in E,\ \forall \lambda \in k,\ u(\lambda x) = \sigma(\lambda)u(x)$.

■ **Exemple 3.1** Si M est une matrice de $\mathrm{M}_n(\mathbb{C})$ alors l'application $\mathbb{C}^n \ni X \mapsto \overline{MX} \in \mathbb{C}^n$ est une application semi-linéaire. ■

R Si $u \neq 0$ alors σ est unique, on le note σ_u. Vérifier que $\sigma_{u\circ v} = \sigma_u \circ \sigma_v$

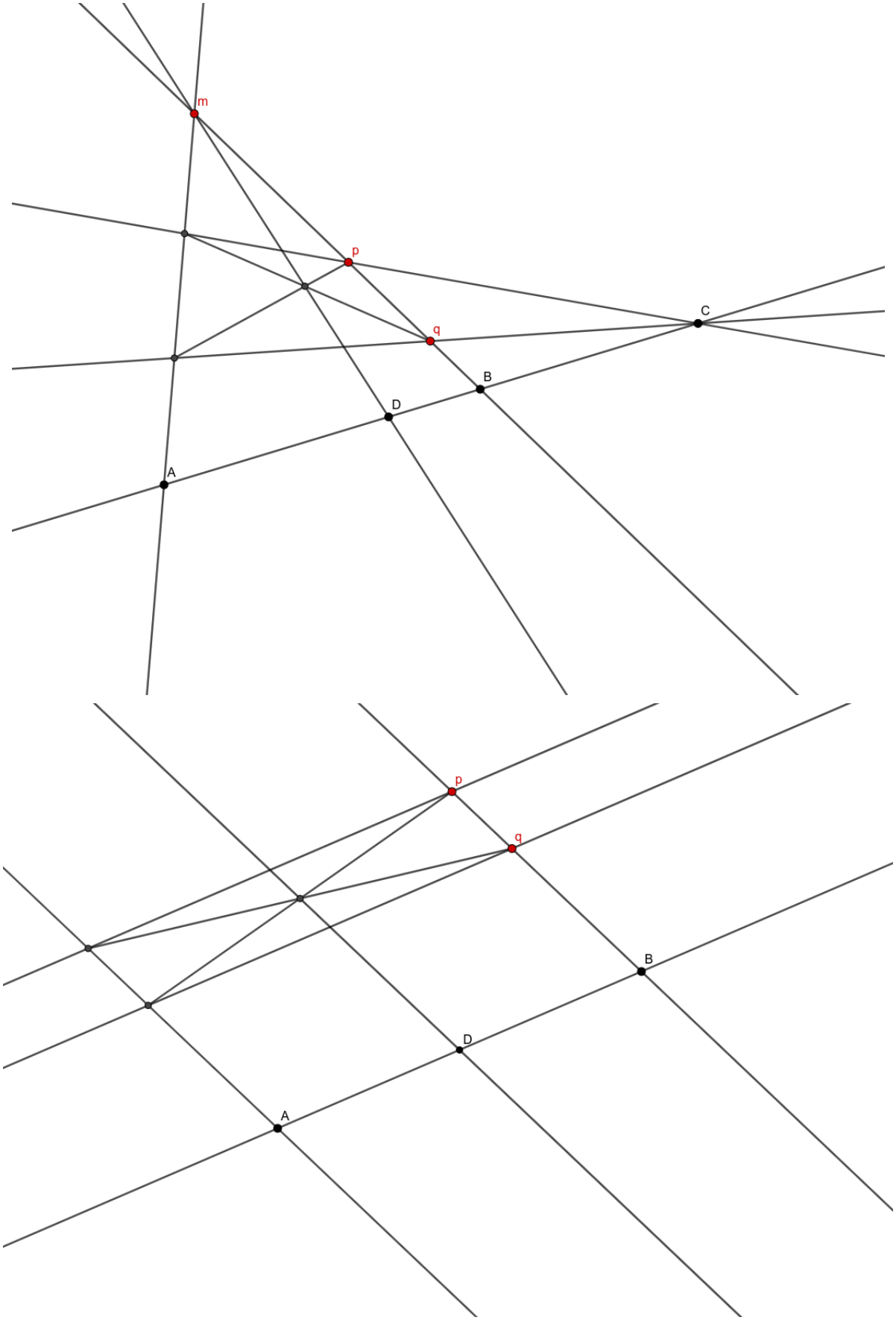

FIGURE 3.15 – Construction du 4ème harmonique

R On a un morphisme du groupe des isomorphismes semi-linéaires vers le groupe des automorphismes de k donnée par $u \mapsto \sigma_u$. Le noyau de ce morphisme est le groupe linéaire. *Remarque pour moi-même :* la suite exacte :

$$1 \to \mathrm{PGL}(E) \to \mathrm{P\Gamma L}(E) \to \mathrm{Aut}(k) \to 1$$

ainsi définie est scindée et non-triviale. Pour définir un scindement il faut choisir une base. Ce qui explique que l'on ne peut pas définir l'action de $\mathrm{Aut}(k)$ sur l'espace projectif sans choisir une base. Tout comme on ne peut pas définir l'action du groupe linéaire sur un espace affine sans choisir un point base.

Le théorème suivant est donné à titre culturel.

Théorème VII.1 Si $k \neq \mathbb{F}_2$ et $d \geqslant 2$ alors toute collinéation est donnée par un isomorphisme semi-linéaire.

Exercice 3.5 Montrer que :

1. Montrer que tout automorphisme de $\mathbb{Q}$ ou $\mathbb{F}_p$ est trivial.
2. Montrer que tout automorphisme continu de $\mathbb{R}$ est trivial.
3. Montrer que tout automorphisme continu de $\mathbb{C}$ est trivial ou la conjugaison.
4. Montrer que tout automorphisme de $\mathbb{R}$ est continu (donc trivial). *Ind. Montrer que tout automorphisme de $\mathbb{R}$ préserve l'ensemble des carrés, donc préserve l'ordre, donc la topologie...*
5. *** Il existe (plein) d'automorphismes de $\mathbb{C}$ non-continus.
   `http://math.ucr.edu/~res/progeom/oldversions/pgnotesappd.pdf`

■

Corollaire VII.2 Toute collinéation de $k\mathbb{P}^d$ avec $d \geqslant 2$ et $k = \mathbb{F}_p$ p premier impair, $k = \mathbb{Q}$ ou $k = \mathbb{R}$ est une homographie. Toute collinéation continue de de $\mathbb{C}\mathbb{P}^d$ avec $d \geqslant 2$ est une homographie ou une anti-homographie (i.e. l'automorphisme de $\mathbb{C}$ est la conjugaison complexe).

VIII La droite projective complexe

R On peut voir $\mathbb{C}$ d'au moins deux façons différentes lorsque l'on fait de la géométrie. On peut voir $\mathbb{C} = \mathbb{R}^2$ comme un espace vectoriel réel de dimension 2 mais alors on voit $\mathbb{C}$ comme un plan affine réel et sa complétion naturelle est alors le plan projectif réel $\mathbb{RP}^2$. Mais on peut aussi voir $\mathbb{C}$ comme un espace vectoriel complexe de dimension 1 et sa complétion naturelle est alors $\mathbb{CP}^1$.

Remarquer bien que dans le premier cas, l'infini est une droite projective réelle, dans le cas l'infini est juste un point.

Ces deux constructions cohabitent sans souci et peuvent même se compléter.

1. Birapport et cercles

Proposition VIII.1 Le birapport de 4 points alignés sur une droite affine réelle contenue dans $\mathbb{C}$ coïncide avec leur birapport comme points de la droite projective complexe $\mathbb{CP}^1$.

Démonstration. Soient a, b, c, d 4 points alignés sur une droite affine réel D de $\mathbb{C}$. Le groupe Is engendré par les rotations et les translations de $\mathbb{R}^2$ est à la fois un sous-groupe des

transformations affines de $\mathbb{R}^2$ donc un sous-groupe de $\mathrm{PGL}_3(\mathbb{R}) = \mathrm{Aut}(\mathbb{RP}^2)$ et **aussi** un sous-groupe des similitudes de $\mathbb{C}$ donc un sous-groupe de $\mathrm{PGL}_2(\mathbb{C}) = \mathrm{Aut}(\mathbb{CP}^1)$. Quitte à appliquer un élément de Is, on peut supposer que la droite D est l'axe réel. Il existe une unique homographie f de $\mathrm{PGL}_2(\mathbb{R})$ qui envoie a sur ∞, b sur 0 et c sur 1. Mais $\mathrm{PGL}_2(\mathbb{R}) \leqslant \mathrm{PGL}_2(\mathbb{C})$ donc f est aussi l'unique homographie de $\mathrm{PGL}_2(\mathbb{C})$ qui envoie a sur ∞, b sur 0 et c sur 1. Par conséquent :

$$[a,b,c,d]_{\mathbb{C}} = f(d) = [a,b,c,d]_{\mathbb{R}} \in \mathbb{R} \cup \{\infty\}$$

■

Corollaire VIII.2 Le birapport de 4 points alignés de $\mathbb{C}$ sur une droite affine réelle est un nombre réel ou l'infini.

Définition VIII.1 On dit que n points de $\mathbb{C}$ sont *cocycliques* lorsqu'il existe un cercle qui les contient.

R On rappelle que 3 points d'un plan réel sont alignés ou bien cocycliques. *Le point de concours des médiatrices est le centre du cercle circonscrit.*

Proposition VIII.3 — Avatar du théorème de l'angle inscrit. Soient $a,b,c \in \mathbb{C}$ non alignés. Soit un point $d \in \mathbb{C}$ différent de a,b,c. Les assertions suivantes sont équivalents :

- Le point d est sur le cercle passant par a,b,c.
- les angles de droites $(ca,cb) = (da,db) \quad [\pi]$ sont égaux.
- Les angles de vecteurs $2(\overrightarrow{ca},\overrightarrow{cb}) = 2(\overrightarrow{da},\overrightarrow{db}) \quad [2\pi]$ sont égaux.

Démonstration. Lire la page wikipedia : `https://fr.wikipedia.org/wiki/Th%C3%A9or%C3%A8me_de_l%27angle_inscrit_et_de_l%27angle_au_centre` ■

Corollaire VIII.4 Le birapport de 4 points de $\mathbb{C}$ est réel (inclus infini) si et seulement si ses 4 points sont alignés ou cocycliques.

Démonstration. On peut supposer les 4 points distincts car sinon ils sont alignés ou cocycliques et leur birapport est $0,1$ ou ∞. On rappelle que :

$$(\overrightarrow{ca},\overrightarrow{cb}) = \mathrm{Arg}\left(\frac{c-b}{c-a}\right) \quad [2\pi]$$

Par conséquent, les points a,b,c,d sont alignés si et seulement si :

$$2\mathrm{Arg}\left(\frac{c-b}{c-a}\right) = 2\mathrm{Arg}\left(\frac{d-b}{d-a}\right) \quad [2\pi]$$

ssi :

$$2\mathrm{Arg}\left(\frac{(d-b)(c-a)}{(d-a)(c-b)}\right) = 0 \quad [2\pi]$$

ssi

$$2\mathrm{Arg}([a,b,c,d]) = 0 \quad [2\pi]$$

ssi

$$\mathrm{Arg}([a,b,c,d]) = 0 \quad [\pi]$$

Autrement dit, ssi $[a,b,c,d] \in \mathbb{R}$. ■

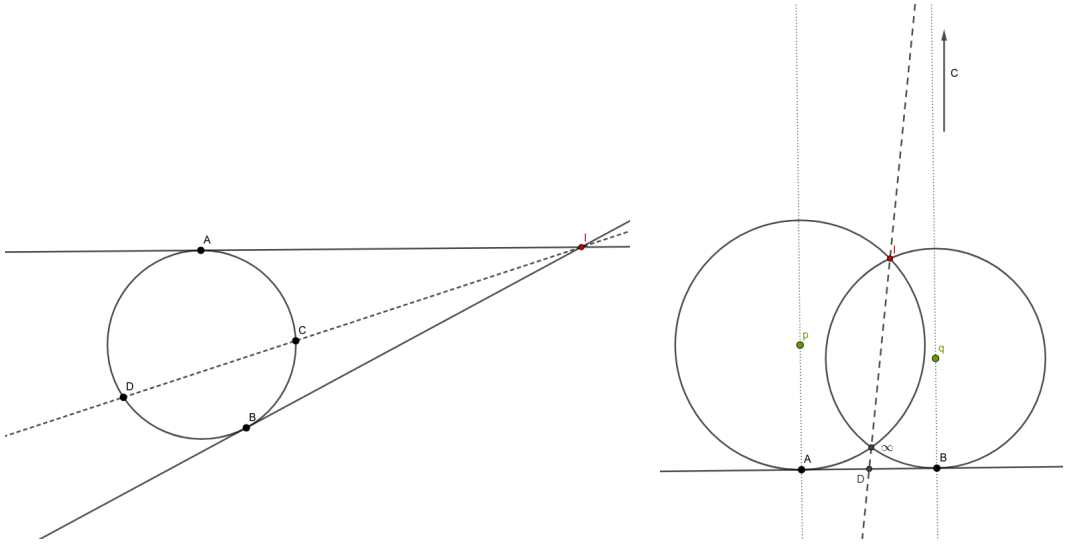

FIGURE 3.16 – Construction du 4ème harmonique

Corollaire VIII.5 Tout élément du groupe $\mathrm{PGL}_2(\mathbb{C})$ envoie une droite ou un cercle sur une droite ou un cercle.

R Il est important de penser à une droite comme à un cercle passant par l'infini. *Noter que c'est cohérent avec la vision compactification d'Alexandrov.*

2. Construction du 4ème harmonique dans $\mathbb{CP}^1$

Proposition VIII.6 Soient a,b,c trois points de $\mathbb{C}$. Si a,b,c ne sont pas alignés alors la construction indiquée dans la figure 3.16 construit l'unique point $d \in \mathbb{C}$ tel que (a,b,c,d) est un quadruplet harmonique.

R Si les points a,b,c sont alignés alors la construction précédente indiquée dans la figure 3.15 construit l'unique point d tel que (a,b,c,d) est un quadruplet harmonique.

Il s'agit d'un exemple d'utilisation de "dans un cas $\mathbb{C}$ est un plan réel, dans un autre cas $\mathbb{C}$ est une droite complexe".

Lemma VIII.7 — Puissance d'un point par rapport à un cercle. Soit M un point et Γ un cercle. Soit d une droite contenant M et rencontrant Γ en A et B (éventuellement $A = B$ si d est tangente à Γ). La quantité $\overrightarrow{MA} \cdot \overrightarrow{MB}$ est indépendante de d et s'appelle la *puissance de M par rapport à Γ*, on la note $P_\Gamma(M)$ et on a $P_\Gamma(M) = OM^2 - R^2$, où O est le centre de Γ et R son rayon.

Démo du Lemme. C'est un calcul utilisant le produit scalaire et le théorème de Pythagore.

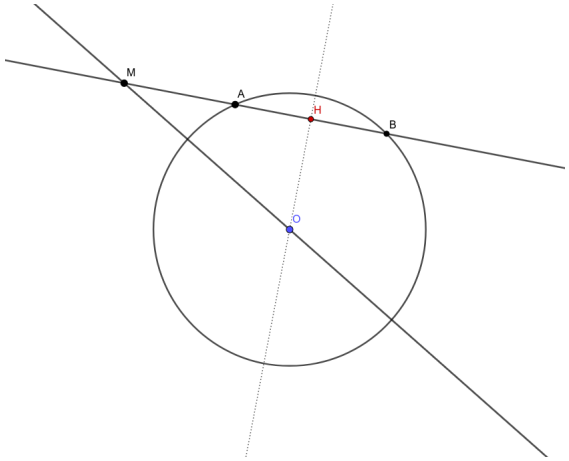

FIGURE 3.17 – Puissance d'un point par rapport à un cercle

On définit $H = (A+B)/2$ et on remarque (OH) est la médiatrice de $[AB]$. On se lance :

$$\begin{aligned}
\overrightarrow{MA}\cdot\overrightarrow{MB} &= (\overrightarrow{MH}+\overrightarrow{HA})\cdot(\overrightarrow{MH}+\overrightarrow{HB}) \\
&= MH^2 - HA^2 && \text{car H le milieu de } [AB] \\
&= MH^2 - (OA^2 - OH^2) && \text{Pythagore dans } OAH \\
&= MH^2 + OH^2 - OA^2 && \text{Pythagore dans } MOH \\
&= MO^2 - R^2
\end{aligned}$$

Remarque : le calcul est bon si M est à l'intérieur du cercle ou si $A = B$. ■

Démo de la proposition. On envoie le point c à l'infini. Le cercle passant par a, b, c devient une droite (ab). Les droites (ma) et (mb) deviennent des cercles Γ, Γ' tangents à (ab) en a et b ; et qui s'intersectent en m et ∞ (ancien point à l'infini). Il faut à présent montrer que $(m\infty) \cap (ab)$ est le milieu de $[ab]$. Pour cela, on utilise la puissance d'un point par rapport à un cercle.

On a $P_\Gamma(d) = P_{\Gamma'}(d)$ puisque $\Gamma \cap \Gamma' = \{m, \infty\}$ et $d \in (m\infty)$. Enfin, $P_\Gamma(d) = da^2$ et $P_\Gamma(d) = db^2$, par suite d est le milieu de $[ab]$. ■

3. Le groupe circulaire

Définition VIII.2 Le *groupe circulaire* est le sous-groupe des homéomorphismes de $\mathbb{CP}^1$ engendré par $\mathrm{PGL}_2(\mathbb{C})$ et la conjugaison complexe.

Théorème VIII.8 Une bijection de $\mathbb{CP}^1$ qui préserve l'ensemble des droites et des cercles est une transformation du groupe circulaire.

Démonstration. Soit f une telle bijection qui à post-composer f par une homographie, on peut supposer que $f(\infty) = \infty$. Ainsi, f envoie une droite sur une droite et un cercle sur un cercle. La construction du quatrième harmonique dans $\mathbb{C}$ se fait uniquement à l'aide de cercles et de droites. On obtient ainsi que si $[a,b,c,d] = -1$ alors $[f(a), f(b), f(c), f(d)] = -1$ (on dit que f *préserve les divisions harmoniques*).

Quitte à composer f par une similitude, on peut supposer que $f(0) = 0$ et $f(1) = 1$. Le lemme suivant montre f est une automorphisme du corps $\mathbb{C}$.

De plus, f préserve l'axe réel $(=(01))$. Par conséquent, f est l'identité ou la conjugaison complexe. ■

Lemma VIII.9 Une bijection $\varphi : \mathbb{C} \to \mathbb{C}$ qui fixe 0 et 1 et préserve les divisions harmoniques est un automorphisme du corps $\mathbb{C}$.

Démonstration. On commence par montrer que f est additive. De l'équivalence $[a,b,c,\infty] = -1 \quad \Leftrightarrow \quad c$ est le milieu de $[ab]$. On en tire que f préserve les milieux, autrement dit :

$$\forall a,b,\in \mathbb{C}, \quad f\left(\frac{a+b}{2}\right) = \frac{f(a)+f(b)}{2}$$

En particulier,

$$\forall a \in \mathbb{C}, \quad 2f(\frac{a}{2}) = f(a)$$

Donc :

$$\forall a,b,\in \mathbb{C}, \quad f(a+b) = f(a)+f(b)$$

Ensuite, on montre que f préserve les carrés. On part de l'égalité :

$$\forall a \in \mathbb{C}, \quad [a,-a,a^2,1] = -1$$

Par conséquent,

$$\forall a \in \mathbb{C}, \quad -1 = [a,-a,a^2,1] = [f(a),-f(a),f(a)^2,1] = [f(a),f(-a),f(a^2),f(1)] = [f(a),-f(a),f(a^2),1]$$

Donc

$$\forall a \in \mathbb{C}, \quad f(a^2) = f(a)^2$$

Enfin, on se rappelle de l'égalité :

$$\forall a,b,\in \mathbb{C}, \quad ab = \frac{1}{4}\left((a+b)^2-(a-b)^2\right)$$

Qui nous montre en utilisant la conservation des milieux, des carrés et l'additivité que :

$$\forall a,b,\in \mathbb{C}, \quad f(ab) = f(a)f(b).$$

■

Fin du cours 10

4. Le groupe linéaire : simplicité

Biblio : on passe au Perrin.

I Déterminant et groupe $\mathrm{SL}(E)$ (Rappel)

L'application déterminant est un morphisme surjectif $\det : \mathrm{GL}(E) \to k^*$. Son noyau s'appelle le groupe *spécial linéaire* et se note $\mathrm{SL}(E)$. On note $\mathrm{SL}_n(k)$ lorsque $E = k^n$.

Proposition I.1 La suite exacte :

$$1 \to \mathrm{SL}(E) \to \mathrm{GL}(E) \to k^* \to 1$$

est scindée. Par conséquent, $\mathrm{GL}(E)$ est le produit semi-direct de $\mathrm{SL}(E)$ par k^*.

Démo à ne pas faire en cours. Les matrices :

$$A(\lambda) = \begin{pmatrix} \lambda & & & \\ & 1 & & 0 \\ & & \ddots & \\ & 0 & & \ddots \\ & & & & 1 \end{pmatrix}$$

fournissent un morphisme $k^* \to \mathrm{GL}(E)$ qui est une section de det. ∎

II Transvection et dilatation

1. C'est quoi ?

Soit $g \in \mathrm{GL}(E)$. Le théorème du rang montre que :

$$\dim \ker(g-1) + \dim \mathrm{Im}\,(g-1) = \dim E$$

On va s'intéresser au automorphisme linéaire qui vérifie $\dim\ker(g-1) = \dim E - 1$ car ce sont eux qui ont le plus de points fixes, ce sont donc les transformations les plus simples de E. Elles vont jouer le rôle que jouaient les transpostions et 3-cycles dans le groupe des permutations.

Définition II.1 Soit $g \in \mathrm{GL}(E)$, $g \neq 1$. Supposons que $H = \ker(g-1)$ est un hyperplan. Les assertions suivantes sont équivalentes :

1. $\det g = \lambda \neq 1$
2. g admet une valeur propre $\lambda \neq 1$ et g est diagonalisable.
3. $\mathrm{Im}\,(g-1) \notin \ker(g-1)$
4. Dans une base convenable g s'écrit :

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

avec $\lambda \neq 1$.

Dans ce cas, g est **la** *dilatation* d'hyperplan $H = \ker(g-1)$, de droite $D = \mathrm{Im}\,(g-1)$, de rapport λ. Les assertions suivantes sont équivalentes :

1. $\det g = 1$
2. g n'est pas diagonalisable.
3. $\mathrm{Im}\,(g-1) \subset \ker(g-1)$
4. Il existe un couple (f,a) tel que $a \in \ker f$ tel que :

$$g(x) = x + f(x)a =: \tau_{f,a}(x)$$

5. Dans une base convenable g s'écrit :

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

Dans ce cas, g est **une** *transvection* d'hyperplan H et de droite $D \subset H$.

Démonstration.

- $4) \Rightarrow 1)$ est trivial.
- $1) \Rightarrow 2)$. Puisque 1 est valeur propre d'ordre $n-1$, $\det(g) = \lambda \neq 1$ est la valeur propre manquante. Nécessairement, la droite propre correspondante n'est pas inclus dans l'hyperplan propre $\ker(g-1)$ donc g est diagonalisable.
- $2) \Rightarrow 3)$, soit x un vecteur propre pour la valeur propre $\lambda \neq 1$, on a :

$$(g-1)(x) = (\lambda-1)x \neq 0 \quad \text{et} \quad x \notin H$$

donc $x \in \mathrm{Im}\,(g-1)$ et donc $\mathrm{Im}\,(g-1) \notin \ker(g-1)$.
- $3) \Rightarrow 4)$, on a $\dim \mathrm{Im}\,(g-1) = 1$, on se donne $e_1, \ldots, e_n$ une base adaptée à la décomposition $\mathrm{Im}\,(g-1) \oplus \ker(g-1) = E$. On rappelle que $\mathrm{Im}\,(g-1), \ker(g-1)$ sont des espaces stables de g, par conséquent, il existe $\mu \neq 0$ tel que $g(e_1) - e_1 = \mu e_1$. Ainsi, $g(e_1) = (1+\mu)e_1$...

- $5) \Rightarrow 1) \Rightarrow 2)$ sont triviales.
- $2) \Rightarrow 5)$ si g n'est pas diagonalisable alors g est conjugué à une somme de bloc de Jordan unipotent. Chaque bloc de Jordan de taille k fournit 1 vecteur de $\ker(g-1)$. On a donc aucun bloc de taille supérieure ou égale à 3 et au plus un bloc de taille 2. On doit donc avoir $n-2$ blocs de jordan triviaux et 1 bloc de taille 2. Soit la forme annoncée en 5.
- $5) \Rightarrow 3)$ trivial.
- $3) \Rightarrow 4)$, soit f une forme linéaire tel que $\ker f = \ker(g-1)$, soit x_0 tel que $f(x_0) = 1$. L'élément $a = g(x_0) - x_0$ est dans l'image de $g-1$ donc dans $\ker(g-1)$. Comme $x_0 \notin \ker(g-1)$, $a \neq 0$. Les applications linéaires g et

$$x \mapsto x + f(x)a$$

  coïncident sur $\ker(g-1)$ et sur $x_0 \notin \ker(g-1)$ donc elles sont égales.
- $4) \Rightarrow 5)$, on prend $e_1 = a$, on complète en une base $(e_1, e_3, \dots, e_n)$ de $\ker f$, ensuite on choisit e_2 tel que $f(e_2) = 1$.

■

R Dans la carte affine d'hyperplan à l'infini H, une transvection est une translation. Inversement, toute translation d'un espace affine se prolonge en une transvection de sa complétion projective.

R Si $\tau : E \to E$ est une transvection d'hyperplan H, soit U un supplémentaire de H, autrement dit $E = H \oplus U$. On choisit $\mathcal{H}$ un hyperplan affine non linéaire parallèle à H. On rappelle que l'on a :

$$\mathbb{P}(E) = \mathcal{H} \sqcup \mathbb{P}(H)$$

et on note $f = \mathbb{P}(\tau)$. Alors :

- f préserve $\mathbb{P}(H)$ et $\mathcal{H}$.
- Mieux, τ préserve $\mathcal{H} = H \times \{1\}$ car τ est une transvection, donc $\tau(e_n) = e_n + \sum_{i=1}^{n-1} \lambda_i e_i$, [1] sinon le déterminant de τ ne serait pas égale à 1.
- L'application induite par f sur $\mathbb{P}(H) = \mathbb{P}(\ker(\tau - 1))$ est l'identité.
- L'application $\varphi : \mathcal{H} \to \mathcal{H} := f_{|\mathcal{H}}$ induite par f sur $\mathcal{H}$ est une application affine qui vérifie :

$$\overrightarrow{\varphi} = \tau_{|H} = \mathrm{Id}$$

- L'application $\varphi : \mathcal{H} \to \mathcal{H}$ est donc une translation.

R Soit φ une translation d'un espace affine $\mathcal{H}$ dirigé par H. Le complété projectif de $\mathcal{H}$ est l'espace projectif $\mathbb{P}(H \oplus k)$. On réalise $\mathcal{H}$ dans $\mathbb{P}(H \oplus k)$, comme $\mathcal{H} = H \times \{1\}$. Il existe un unique automorphisme linéaire τ tel que :

- $\mathbb{P}(\tau)_{|\mathcal{H}} = \varphi$.
- $\tau(\mathcal{H}) = \mathcal{H}$.

Cet automorphisme τ est une transvection. En effet, $\tau_{|H} = \overrightarrow{\varphi} = \mathrm{Id}$. Par conséquent, $\ker(\tau - 1)$ est un hyperplan. On remarque que la normalisation $\tau(\mathcal{H}) = \mathcal{H}$ force à avoir $\det(\tau) = 1$ [2], donc τ est une transvection.

1. où e_n est le dernier vecteur d'une base $(e_i)_i$ adaptée à $H \oplus k$

2. Pour ceux qui préfère les matrices, la normalisation $\tau(\mathcal{H}) = \mathcal{H}$ force à avoir $\tau(e_n) = e_n + \sum_{i=1}^{n-1} \lambda_i e_i$, où e_n est le dernier vecteur d'une base $(e_i)_i$ adaptée à $H \oplus k$.

R La donnée de (H,D,λ) caractérise la dilation. La donnée de (H,D) ne caractérise pas la transvection. Les transvections :

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

ont les mêmes H et D. Par contre, la donnée de (f,a) caractérise g, la réciproque est fausse : $\tau_{f,a} = \tau_{\lambda f, a/\lambda}$. Et, c'est la seule erreur possible (exo).

R On a $\tau_{f,a} \circ \tau_{f,b} = \tau_{f,a+b}$. En particulier, l'inverse de la transvection $\tau_{f,a}$ est la transvection $\tau_{f,-a}$.

R Si $a \notin \ker(f)$, l'application linéaire $x \mapsto x + f(x)a$ est une dilation d'hyperplan $\ker(f)$, de droite $\langle a \rangle$ et de rapport 2.

2. Conjugaison des dilatations et des transvections

Corollaire II.1

- Les dilatations de rapport λ sont conjuguées dans $\mathrm{GL}(E)$.
- Inversement, deux dilations sont conjuguées si et seulement si elles ont le même rapport.
- Les transvections sont conjugués dans $\mathrm{GL}(E)$.

Démonstration. Même réduite de Jordan ! C'est un corollaire du point 4, resp. 5. ∎

On pose :

$$J_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad J_\lambda^n = J_\lambda \oplus \mathrm{Id}_{n-2}$$

Proposition II.2

- Si $n \geqslant 3$ alors les transvections sont conjuguées dans $\mathrm{SL}_n(k)$.
- Dans $\mathrm{SL}_2(k)$, toute transvection est conjuguée à J_λ pour un certain $\lambda \in k^*$.
- Dans $\mathrm{SL}_2(k)$, si $\lambda, \mu \in k^*$ alors J_λ et J_μ sont conjuguées ssi λ/μ est un carré.

R Les classes de conjugaison des transvections dans $\mathrm{SL}_2(k)$ sont donc en bijection avec le groupe k^*/k^{*2}. On peut montrer que :

$$\mathbb{C}^*/\mathbb{C}^{*2} = \{1\} \quad \mathbb{R}^*/\mathbb{R}^{*2} = \{\pm 1\} \quad \#\mathbb{F}_q^*/\mathbb{F}_q^{*2} = 2 \quad \mathbb{F}_{2^\alpha}^*/\mathbb{F}_{2^\alpha}^{*2} = \{1\} \quad \#\mathbb{Q}^*/\mathbb{Q}^{*2} = \infty$$

pour $q = p^\alpha$ avec p premier impair.

Démonstration. Cas $n \geqslant 3$. Soit u une transvection, il existe $g \in \mathrm{GL}_n(k)$ tel que $gug^{-1} = J_1^n$, on cherche γ tel que $\gamma J_1^n \gamma^{-1} = J_1^n$ et $\det(\gamma g) = 1$. Car ainsi, on aura :

$$(\gamma g)u(\gamma g)^{-1} = \gamma J_1^n \gamma^{-1} = J_1^n \quad \text{et} \quad \gamma g \in \mathrm{SL}_n(k)$$

On prend :

$$\gamma = \begin{pmatrix} \lambda^{-1} & & & & & 0 \\ & \lambda^{-1} & & & & \\ & & \lambda & & & \\ & & & 1 & & \\ & & & & \ddots & \\ 0 & & & & & 1 \end{pmatrix}$$

avec $\lambda = \det(g)$.

Cas $n = 2$. Il existe une base $(\varepsilon_1, \varepsilon_2)$ tel que u a pour matrice J_1. Dans la base $(\alpha\varepsilon_1, \varepsilon_2)$, la matrice de u est de la forme J_λ. On peut choisir α tel que $\det(\alpha\varepsilon_1, \varepsilon_2) = 1$.

Supposons qu'il existe $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $ad - bc = 1$ tel que $gJ_\lambda = J_\mu g$. On calcule :

$$gJ_\lambda = \begin{pmatrix} a & b + a\lambda \\ c & d + c\lambda \end{pmatrix} = J_\mu g = \begin{pmatrix} a + \mu c & b + \mu d \\ c & d \end{pmatrix}$$

On obtient donc :

$$\mu c = 0 \qquad a\lambda = \mu d \qquad c\lambda = 0$$

Donc :

$$c = 0 \qquad ad = 1 \qquad \lambda/\mu = d/a = d^2$$

Réciproquement, si $\lambda/\mu = \delta^2$ est un carré, la matrice g avec $d = \delta$, $a = d^{-1}$, $c = 0$, b quelconque, do the job. ■

3. Centres de $\mathrm{GL}_n(k)$ et $\mathrm{SL}_n(k)$

Proposition II.3 La transformation linéaire $gT_{f,a}g^{-1}$ est la transvection $T_{f\circ g^{-1}, g(a)}$.

Démonstration.

$$gT_{f,a}g^{-1}x = gT_{f,a}\left(g^{-1}x\right) = g\left(g^{-1}x + f(g^{-1}x)a\right) = x + f\circ g^{-1}(x)g(a)$$

■

Proposition II.4 Le centre de $\mathrm{GL}(E)$ est le groupe des homothéties, le centre de $\mathrm{SL}(E)$ est le groupe des homothéties de déterminant 1. Ce dernier est isomorphe à $\mu_n(k)$ le groupe des racines énièmes de l'unité de k.

Démonstration. Soit $g \in \mathrm{GL}(E)$ qui commutent avec tous les éléments de $\mathrm{SL}(E)$. En particulier, g commute avec tous les transvections. Par conséquent, on a pour tout (f, a) avec $a, f \neq 0$ et $f(a) = 0$:

$$T_{f\circ g^{-1}, g(a)} = gT_{f,a}g^{-1} = T_{f,a}$$

En particulier, on doit avoir $g(a)$ et a colinéaires, et ceux pour tout $a \in E$. On en déduit que g est une homothétie. ■

4. Génération

Définition II.2

- On note E_{ij} la matrice qui ne contient que des zéros sauf un 1 à la ligne i et à la colonne j.
- Les matrices E_{ij} s'appellent les *matrices élémentaires*.
- Les matrices $T_{ij}(\lambda) := I + \lambda E_{ij}$, pour $i \neq j$ s'appellent les *transvections élémentaires*.
- Les matrices $I + (\lambda - 1)E_{ii}$ s'appellent les *dilatations élémentaires*.

Proposition II.5 Les transvections élémentaires engendrent $\mathrm{SL}_n(k)$

Démonstration. La multiplication à gauche (resp. à droite) par la matrice de transvection élémentaire $T_{ij}(\lambda)$ revient à effectuer l'opération élémentaire $L_i \leftarrow L_i + \lambda L_j$ (resp. $C_j \leftarrow C_j + \lambda C_i$).

Notons qu'il est possible de réaliser l'échange de deux lignes (ou de deux colonnes) uniquement à l'aide de transvections modulo un changement de signe : en effet, la matrice $T_{ij}(1)T_{ji}(-1)T_{ij}(1)$ a pour effet (par multiplication à gauche) de remplacer L_i par L_j et L_j par $-L_i$, les autres lignes étant invariantes [3].

Soit $g \in \mathrm{SL}_n(k)$. On applique l'algorithme du pivot de Gauss. Comme g est inversible, sa première colonne n'est pas nulle. Quitte à échanger deux lignes (c'est à dire à appliquer des transvections élémentaires à gauche), on peut supposer que le coefficient $a_{21} \neq 0$.

On commence par utiliser le pivot $(1,2)$. On réalise l'opération $L_1 \leftarrow L_1 - \frac{g_{11}-1}{g_{12}} L_2$ qui permet de se ramener à la situation $g_{11} = 1$, en appliquant une transvection. Ensuite, on utilise le pivot $(1,1)$, $2(n-1)$ fois pour se ramener à $g_{i1} = 0$ et $g_{1i} = 0$ pour $i \geqslant 2$.

Autrement dit, ils existent $t_1, \ldots, t_p$ et $u_1, \ldots, u_q$ des transvections tel que :

$$t_1 \cdots t_p g u_1 \cdots u_q = \begin{pmatrix} 1 & 0 \\ 0 & h \end{pmatrix}$$

où $h \in \mathrm{SL}_{n-1}(k)$. Par récurrence, on obtient qu'ils existent $t_1, \ldots, t_p$ et $u_1, \ldots, u_q$ des transvections tel que :

$$t_1 \cdots t_p g u_1 \cdots u_q = 1$$

Par suite, g est un produit de transvections. ∎

Corollaire II.6 Les transvections élémentaires et les dilatations élémentaires engendrent $\mathrm{GL}_n(k)$.

III Groupe dérivé

Proposition III.1 Si $n \geqslant 2$ et $(n,k) \neq (2,\mathbb{F}_2), (2,\mathbb{F}_3)$ alors toute transvection élémentaire est un commutateur de $\mathrm{SL}_n(k)$.

Démonstration. L'automorphisme $g \mapsto g^{-T}$, échange les transvections élémentaires triangulaires inférieures avec les supérieures. On se concentre donc sur les supérieures.

3. Il n'est évidemment pas possible de réaliser l'échange de deux lignes sans apparition de ce signe – puisque cette opération change le signe du déterminant.

Il faut distinguer les cas $n \geqslant 3$ du cas $n = 2$. Pour $n \geqslant 3$, on fait le calcul suivant dans $\mathrm{SL}_3(k)$, on a :

$$\left[\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}, \begin{pmatrix}1&0&0\\0&1&x\\0&0&1\end{pmatrix}\right] = \begin{pmatrix}1&0&x\\0&1&0\\0&0&1\end{pmatrix}$$

Autrement dit $[T_{12}(1), T_{23}(x)] = T_{13}(x)$. De façon général, on a :

$$[T_{ij}(1), T_{jk}(x)] = T_{ik}(x)$$

D'où le résultat.

Pour $n = 2$, le résultat est faux pour $\#k = 2,3$ donc il faut faire plus attention... On fait le calcul suivant :

$$\left[\begin{pmatrix}1&y\\0&1\end{pmatrix}, \begin{pmatrix}x&0\\0&x^{-1}\end{pmatrix}\right] = \begin{pmatrix}1&y(1-x^2)\\0&1\end{pmatrix}$$

Ainsi, si on peut trouver un $x \in k^*$ tel que $x^2 \neq 1$ alors toutes les transvections élémentaires seront des commutateurs [4]. L'équation $x^2 = 1$ possède au plus 2 solutions dans un corps, donc si $\#k \geqslant 4$ alors on peut trouver un tel x. ■

R [Rappel] Un groupe G est parfait lorsque $G = G'$.

Exercice 4.1 Tout quotient d'un groupe parfait est parfait. ■

Corollaire III.2 Si $n \geqslant 2$ et $(n,k) \neq (2,\mathbb{F}_2), (2,\mathbb{F}_3)$ alors :
- les groupes $\mathrm{SL}_n(k)$ et $\mathrm{PSL}_n(k)$ sont parfaits.
- $D(\mathrm{GL}_n(k)) = \mathrm{SL}_n(k)$.
- $D(\mathrm{PGL}_n(k)) = \mathrm{PSL}_n(k)$.

Démonstration. On vient de voir que les transvections élémentaires sont des commutateurs et on a vu précédemment qu'elles engendraient $\mathrm{SL}_n(k)$. D'où le résultat pour les $\mathrm{SL}_n(k)$.

L'exo quotient d'un groupe parfait montre le résultat pour les $\mathrm{PSL}_n(k)$.

Clairement,

$$\mathrm{SL}_n(k) = D(\mathrm{SL}_n(k)) \leqslant D(\mathrm{GL}_n(k)) \leqslant \mathrm{SL}_n(k)$$

D'où le résultat pour les $\mathrm{GL}_n(k)$. On fait de même pour les $\mathrm{PGL}_n(k)$. ■

R [Le cas $(n,k) = (2,\mathbb{F}_2)$] On rappelle que :

$$\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$$

Le groupe dérivé de $\mathrm{XL}_2(\mathbb{F}_2)$ est donc un sous-groupe propre non-trivial sans nom qui correspond à $\mathfrak{A}_3$.

4. Au passage on remarque que dans $\mathbb{F}_2$ et $\mathbb{F}_3$, on a $x^2 = 1$ pour tout $x \neq 0$.

R [Le cas $(n,k) = (2,\mathbb{F}_3)$]

$$\sharp \mathrm{GL}_2(\mathbb{F}_3) = 48 \qquad \sharp \underbrace{\mathrm{SL}_2(\mathbb{F}_3)}_{\neq \mathfrak{S}_4} = 24 \qquad \sharp \underbrace{\mathrm{PGL}_2(\mathbb{F}_3)}_{\simeq \mathfrak{S}_4} = 24 \qquad \sharp \underbrace{\mathrm{PSL}_2(\mathbb{F}_3)}_{\simeq \mathfrak{A}_4} = 12$$

et on a :

1. $D(\mathrm{GL}_2(\mathbb{F}_3)) = \mathrm{SL}_2(\mathbb{F}_3)$. Voir Feuille de TD 3.
2. $D(\mathrm{SL}_2(\mathbb{F}_3)) < \mathrm{SL}_2(\mathbb{F}_3)$ est un sous-groupe d'ordre 8 isomorphe au groupe des quaternions. Voir Feuille de TD 3.
3. $D(\mathrm{PGL}_2(\mathbb{F}_3)) = \mathrm{PSL}_2(\mathbb{F}_3)$, correspond à $\mathfrak{S}_4' = \mathfrak{A}_4$. Voir Chapitre 1.
4. $D(\mathrm{PSL}_2(\mathbb{F}_3)) < \mathrm{PSL}_2(\mathbb{F}_3)$, correspond à $\mathfrak{A}_4' = V$. Voir Feuille de TD 1.

IV Le Lemme d'Iwasawa

Théorème IV.1 — Lemme d'Iwasawa.
Soient G un groupe parfait et une action $G \curvearrowright X$ fidèle, 2-transitive.
On suppose que le stabilisateur G_x d'un point x de X possède un sous-groupe distingué abélien A tel que les conjugués de A dans G engendre G.
Alors G est simple.

R [Rappel] Dans un groupe quelconque, si $K, N \leqslant G$ et $N \lhd G$ alors $\langle N, K\rangle = NK = KN$.

Proposition IV.2 Soit $G \curvearrowright X$ une action 2-transitive. Soit $G_x < H \leqslant G$ alors $H = G$, autrement dit le stabilisateur d'un point est un sous-groupe maximal de G.

Démonstration. Soit $g \in G$. Si $gx = x$ alors $g \in H$ et c'est déjà gagné. Sinon $gx = y \neq x$. Par hypothèse, il existe un $h \in H$ tel que $hx = z \neq x$. Comme l'action est 2-transitive, il existe un $k \in G_x$ tel que $ky = z$. Par suite, $h^{-1}kgx = x$, donc $g \in H$. ∎

Fin du cours 11

Démo du Lemme d'Iwasawa. On fixe un $x \in X$. Soit $N \lhd G$.

Cas 1 : $N \leqslant G_x$ alors :

$$\forall g \in G, \quad N = gNg^{-1} \leqslant gG_xg^{-1} = G_{gx} \qquad \Rightarrow \qquad N \leqslant \bigcap_{y \in X} G_y = \ker(G \curvearrowright X) = \{1\}$$

comme l'action est fidèle et transitive.

On se place à présent dans le cas 2 : $N \not\leqslant G_x$. Par conséquent, le groupe $NG_x = G$ par le lemme de maximalité.

Montrons qu'alors $G = AN$. Tout élément $g \in G$ s'écrit $g = nk$ avec $n \in N$ et $k \in G_x$. Par conséquent, $gAg^{-1} = nkAk^{-1}n^{-1} = nAn^{-1} \leqslant \langle A, N \rangle = AN$, or G est engendré par les conjugués de A. Donc $G \leqslant AN$.

Par conséquent, $G/N = AN/N = A/(A \cap N)$ est abélien, donc $G' \leqslant N$ mais G est parfait donc $G = N$. ∎

V Appliquer le Lemme d'Iwasawa à PSL(V)

Il faut vérifier 3 points

1. L'action $\mathrm{PSL}(V) \curvearrowright \mathbb{P}(V)$ est 2-transitive et fidèle. Déjà fait.
2. Le groupe $\mathrm{PSL}(V)$ est parfait. Déjà fait.
3. Trouver un A qui marche.

On a tout préparé pour montrer facilement le dernier point. Par dualité, le stabilisateur P du point $[e_n]$ pour l'action $\mathrm{PSL}(V) \curvearrowright \mathbb{P}(V)$ est :

$$\begin{aligned} P &= \{g \in \mathrm{PSL}_n(k) \,|\, g \simeq \begin{pmatrix} A & 0 \\ b & \lambda \end{pmatrix}, A \in \mathrm{GL}_{n-1}(k), b \in k^n, \lambda \in k^*, s.t. \det(A)\lambda = 1\} \\ &\simeq \{g \in \mathrm{SL}_n(k) \,|\, g = \begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix}, A \in \mathrm{SL}_{n-1}(k), b \in k^n\} \end{aligned}$$

à l'aide de l'isomorphisme $M \mapsto M^{-T}$ on obtient :

$$\begin{aligned} &\simeq \{g \in \mathrm{SL}_n(k) \,|\, g = \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix}, A \in \mathrm{SL}_{n-1}(k), b \in k^n\} \\ &=: \mathrm{SAff}_{n-1}(k) \end{aligned}$$

En français, le stabilisateur P du point $[e_n]$ pour l'action $\mathrm{PSL}(V) \curvearrowright \mathbb{P}(V)$ est isomorphe au stabilisateur de l'hyperplan $\{x_n = 0\}$. Le stabilisateur d'un hyperplan H est isomorphe au groupe spécial affine sur k^{n-1}.

Le groupe spécial affine possède un sous-groupe abélien distingué : le sous-groupe des translations. Autrement dit, on prend :

$$\begin{aligned} A &= \{g \in \mathrm{PSL}_n(k) \,|\, g \simeq \begin{pmatrix} I & 0 \\ b & \lambda \end{pmatrix}, b \in k^n\} \\ &= \{g \in \mathrm{SL}_n(k) \,|\, g \simeq \begin{pmatrix} I & 0 \\ b & 1 \end{pmatrix}, b \in k^n\} \\ &\simeq k^n \end{aligned}$$

C'est le groupe des transvections de droite $[e_n]$. Or toute transvection est conjugué dans $\mathrm{SL}_n(k)$ à un élément de A. Le groupe $\mathrm{PSL}(V)$ étant engendré par les transvections. On obtient le résultat souhaité.

VI Les isomorphismes exceptionnels

1. Quelques calculs de cardinaux dans le cas des corps fini

Proposition VI.1 Si $k = \mathbb{F}_q$ alors $\mu_n(k)$ le groupe cyclique d'ordre $n \wedge (q-1)$.

Démonstration. Le groupe $\mu_n(k)$ est cyclique car c'est un sous-groupe fini du groupe multiplicatif d'un corps. Soit x_0 un générateur de $\mu_n(k)$, on a :

$$x_0^n = 1 \quad \text{et} \quad x_0^{q-1} \quad \text{donc} \quad x_0^{n\wedge(q-1)}$$

On en déduit que $\sharp\mu_n(k) = \sharp\langle x_0\rangle \,|\, n \wedge (q-1)$ [5].

Inversement, soit y_0 un générateur de $\mathbb{F}_q^\star$. L'ordre de y_0 est $q-1$ [6]. L'élément $x_1 = y_0^{q-1/n\wedge(q-1)}$ est d'ordre $n \wedge (q-1)$ dans $k^\times$. On vérifie que x_1 est aussi d'ordre n :

$$x_1^n = y_0^{n(q-1)/n\wedge(q-1)} = y_0^{(q-1)\times n/n\wedge(q-1)} = \left(y_0^{q-1}\right)^{n/n\wedge(q-1)} = 1^{n/n\wedge(q-1)} = 1$$

Donc, $n \wedge (q-1) \,|\, \sharp\mu_n(k)$, par le théorème de Lagrange. ∎

2. Des ordres... en pagaille

0	2	3	4	5
$\mathbb{F}_2$	$2\cdot 3$	$2^3\cdot 3\cdot 7$	$2^6\cdot 3^2\cdot 5\cdot 7$	$2^{10}\cdot 3^2\cdot 5\cdot 7\cdot 31$
$\mathbb{F}_3$	$2^2\cdot 3$	$2^4\cdot 3^3\cdot 13$	$2^7\cdot 3^6\cdot 5\cdot 13$	$2^9\cdot 3^{10}\cdot 5\cdot 11^2\cdot 13$
$\mathbb{F}_4$	$2^2\cdot 3\cdot 5$	$2^6\cdot 3^2\cdot 5\cdot 7$	$2^{12}\cdot 3^4\cdot 5^2\cdot 7\cdot 17$	$2^{20}\cdot 3^5\cdot 5^2\cdot 7\cdot 11\cdot 17\cdot 31$
$\mathbb{F}_5$	$2^2\cdot 3\cdot 5$	$2^5\cdot 3\cdot 5^3\cdot 31$	$2^7\cdot 3^2\cdot 5^6\cdot 13\cdot 31$	$2^{11}\cdot 3^2\cdot 5^{10}\cdot 11\cdot 13\cdot 31\cdot 71$

	2	3	4	5
$\mathbb{F}_2$	6	168	20160	9999360
$\mathbb{F}_3$	12	5616	6065280	237783237120
$\mathbb{F}_4$	60	20160	987033600	258492255436800
$\mathbb{F}_5$	60	372000	7254000000	56653740000000000
$\mathbb{F}_7$	168	1876896	2317591180800	187035198320488089600
$\mathbb{F}_8$	504	16482816	34558531338240	463822600749101088768 0
$\mathbb{F}_9$	360	42456960	50759843097600	786602807964196134912 00
$\mathbb{F}_{11}$	660	212427600	2069665112592000	195205270856505918624 0000
$\mathbb{F}_{13}$	1092	270178272	12714519233969280	539322992420959314658621440
$\mathbb{F}_{16}$	4080	1425715200	1148120010326016000	157796262193083479123558400 00

5. Cette inégalité est valide sur tout corps.
6. Ceci est vrai car $k^\times$ est cyclique, ce qui provient du fait que k est fini.

0	2	3	4	5
$\mathbb{F}_2$	$2\cdot 3$	$2^3\cdot 3\cdot 7$	$2^6\cdot 3^2\cdot 5\cdot 7$	$2^{10}\cdot 3^2\cdot 5\cdot 7\cdot 31$
$\mathbb{F}_3$	$2^2\cdot 3$	$2^4\cdot 3^3\cdot 13$	$2^7\cdot 3^6\cdot 5\cdot 13$	$2^9\cdot 3^{10}\cdot 5\cdot 11^2\cdot 13$
$\mathbb{F}_4$	$2^2\cdot 3\cdot 5$	$2^6\cdot 3^2\cdot 5\cdot 7$	$2^{12}\cdot 3^4\cdot 5^2\cdot 7\cdot 17$	$2^{20}\cdot 3^5\cdot 5^2\cdot 7\cdot 11\cdot 17\cdot 31$
$\mathbb{F}_5$	$2^2\cdot 3\cdot 5$	$2^5\cdot 3\cdot 5^3\cdot 31$	$2^7\cdot 3^2\cdot 5^6\cdot 13\cdot 31$	$2^{11}\cdot 3^2\cdot 5^{10}\cdot 11\cdot 13\cdot 31\cdot 71$
$\mathbb{F}_7$	$2^3\cdot 3\cdot 7$	$2^5\cdot 3^2\cdot 7^3\cdot 19$	$2^9\cdot 3^4\cdot 5^2\cdot 7^6\cdot 19$	$2^{11}\cdot 3^5\cdot 5^2\cdot 7^{10}\cdot 19\cdot 2801$
$\mathbb{F}_8$	$2^3\cdot 3^2\cdot 7$	$2^9\cdot 3^2\cdot 7^2\cdot 73$	$2^{18}\cdot 3^4\cdot 5\cdot 7^3\cdot 13\cdot 73$	$2^{30}\cdot 3^4\cdot 5\cdot 7^4\cdot 13\cdot 31\cdot 73\cdot 151$
$\mathbb{F}_9$	$2^3\cdot 3^2\cdot 5$	$2^7\cdot 3^6\cdot 5\cdot 7\cdot 13$	$2^{10}\cdot 3^{12}\cdot 5^2\cdot 7\cdot 13\cdot 41$	$2^{15}\cdot 3^{20}\cdot 5^2\cdot 7\cdot 11^2\cdot 13\cdot 41\cdot 61$
$\mathbb{F}_{11}$	$2^2\cdot 3\cdot 5\cdot 11$	$2^4\cdot 3\cdot 5^2\cdot 7\cdot 11^3\cdot 19$	$2^7\cdot 3^2\cdot 5^3\cdot 7\cdot 11^6\cdot 19\cdot 61$	$2^9\cdot 3^2\cdot 5^4\cdot 7\cdot 11^{10}\cdot 19\cdot 61\cdot 3221$
$\mathbb{F}_{13}$	$2^2\cdot 3\cdot 7\cdot 13$	$2^5\cdot 3^2\cdot 7\cdot 13^3\cdot 61$	$2^7\cdot 3^4\cdot 5\cdot 7^2\cdot 13^6\cdot 17\cdot 61$	$2^{11}\cdot 3^5\cdot 5\cdot 7^2\cdot 13^{10}\cdot 17\cdot 61\cdot 30941$
$\mathbb{F}_{16}$	$2^4\cdot 3\cdot 5\cdot 17$	$2^{12}\cdot 3^2\cdot 5^2\cdot 7\cdot 13\cdot 17$	$2^{24}\cdot 3^4\cdot 5^3\cdot 7\cdot 13\cdot 17^2\cdot 257$	$2^{40}\cdot 3^5\cdot 5^4\cdot 7\cdot 11\cdot 13\cdot 17^2\cdot 31\cdot 41\cdot 257$
$\mathbb{F}_{17}$	$2^4\cdot 3^2\cdot 17$	$2^9\cdot 3^2\cdot 17^3\cdot 307$	$2^{13}\cdot 3^4\cdot 5\cdot 17^6\cdot 29\cdot 307$	$2^{19}\cdot 3^4\cdot 5\cdot 17^{10}\cdot 29\cdot 307\cdot 88741$
$\mathbb{F}_{19}$	$2^2\cdot 3^2\cdot 5\cdot 19$	$2^4\cdot 3^4\cdot 5\cdot 19^3\cdot 127$	$2^7\cdot 3^7\cdot 5^2\cdot 19^6\cdot 127\cdot 181$	$2^9\cdot 3^9\cdot 5^2\cdot 19^{10}\cdot 127\cdot 151\cdot 181\cdot 911$
$\mathbb{F}_{23}$	$2^3\cdot 3\cdot 11\cdot 23$	$2^5\cdot 3\cdot 7\cdot 11^2\cdot 23^3\cdot 79$	$2^9\cdot 3^2\cdot 5\cdot 7\cdot 11^3\cdot 23^6\cdot 53\cdot 79$	$2^{11}\cdot 3^2\cdot 5\cdot 7\cdot 11^4\cdot 23^{10}\cdot 53\cdot 79\cdot 292561$
$\mathbb{F}_{25}$	$2^3\cdot 3\cdot 5^2\cdot 13$	$2^7\cdot 3^2\cdot 5^6\cdot 7\cdot 13\cdot 31$	$2^{10}\cdot 3^4\cdot 5^{12}\cdot 7\cdot 13^2\cdot 31\cdot 313$	$2^{15}\cdot 3^5\cdot 5^{20}\cdot 7\cdot 11\cdot 13^2\cdot 31\cdot 71\cdot 313\cdot 521$
$\mathbb{F}_{27}$	$2^2\cdot 3^3\cdot 7\cdot 13$	$2^4\cdot 3^9\cdot 7\cdot 13^2\cdot 757$	$2^7\cdot 3^{18}\cdot 5\cdot 7^2\cdot 13^3\cdot 73\cdot 757$	$2^9\cdot 3^{30}\cdot 5\cdot 7^2\cdot 11^2\cdot 13^4\cdot 73\cdot 757\cdot 4561$
$\mathbb{F}_{29}$	$2^2\cdot 3\cdot 5\cdot 7\cdot 29$	$2^5\cdot 3\cdot 5\cdot 7^2\cdot 13\cdot 29^3\cdot 67$	$2^7\cdot 3^2\cdot 5^2\cdot 7^3\cdot 13\cdot 29^6\cdot 67\cdot 421$	$2^{11}\cdot 3^2\cdot 5^2\cdot 7^4\cdot 13\cdot 29^{10}\cdot 67\cdot 421\cdot 732541$
$\mathbb{F}_{31}$	$2^5\cdot 3\cdot 5\cdot 31$	$2^7\cdot 3^2\cdot 5^2\cdot 31^3\cdot 331$	$2^{13}\cdot 3^4\cdot 5^3\cdot 13\cdot 31^6\cdot 37\cdot 331$	$2^{15}\cdot 3^5\cdot 5^4\cdot 11\cdot 13\cdot 31^{10}\cdot 37\cdot 331\cdot 17351$
$\mathbb{F}_{32}$	$2^5\cdot 3\cdot 11\cdot 31$	$2^{15}\cdot 3\cdot 7\cdot 11\cdot 31^2\cdot 151$	$2^{30}\cdot 3^2\cdot 5^2\cdot 7\cdot 11^2\cdot 31^3\cdot 41\cdot 151$	$2^{50}\cdot 3^2\cdot 5^2\cdot 7\cdot 11^2\cdot 31^4\cdot 41\cdot 151\cdot 601\cdot 1801$
$\mathbb{F}_{37}$	$2^2\cdot 3^2\cdot 19\cdot 37$	$2^5\cdot 3^4\cdot 7\cdot 19\cdot 37^3\cdot 67$	$2^7\cdot 3^7\cdot 5\cdot 7\cdot 19^2\cdot 37^6\cdot 67\cdot 137$	$2^{11}\cdot 3^9\cdot 5\cdot 7\cdot 11\cdot 19^2\cdot 37^{10}\cdot 41\cdot 67\cdot 137\cdot 4271$
$\mathbb{F}_{41}$	$2^3\cdot 3\cdot 5\cdot 7\cdot 41$	$2^7\cdot 3\cdot 5^2\cdot 7\cdot 41^3\cdot 1723$	$2^{10}\cdot 3^2\cdot 5^3\cdot 7^2\cdot 29^2\cdot 41^6\cdot 1723$	$2^{15}\cdot 3^2\cdot 5^4\cdot 7^2\cdot 29^2\cdot 41^{10}\cdot 1723\cdot 579281$
$\mathbb{F}_{43}$	$2^2\cdot 3\cdot 7\cdot 11\cdot 43$	$2^4\cdot 3^2\cdot 7^2\cdot 11\cdot 43^3\cdot 631$	$2^7\cdot 3^4\cdot 5^2\cdot 7^3\cdot 11^2\cdot 37\cdot 43^6\cdot 631$	$2^9\cdot 3^5\cdot 5^2\cdot 7^4\cdot 11^2\cdot 37\cdot 43^{10}\cdot 631\cdot 3500201$
$\mathbb{F}_{47}$	$2^4\cdot 3\cdot 23\cdot 47$	$2^6\cdot 3\cdot 23^2\cdot 37\cdot 47^3\cdot 61$	$2^{11}\cdot 3^2\cdot 5\cdot 13\cdot 17\cdot 23^3\cdot 37\cdot 47^6\cdot 61$	$2^{13}\cdot 3^2\cdot 5\cdot 11\cdot 13\cdot 17\cdot 23^4\cdot 31\cdot 37\cdot 47^{10}\cdot 61\cdot 14621$
$\mathbb{F}_{49}$	$2^4\cdot 3\cdot 5^2\cdot 7^2$	$2^9\cdot 3^2\cdot 5^2\cdot 7^6\cdot 19\cdot 43$	$2^{13}\cdot 3^4\cdot 5^4\cdot 7^{12}\cdot 19\cdot 43\cdot 1201$	$2^{19}\cdot 3^5\cdot 5^4\cdot 7^{20}\cdot 11\cdot 19\cdot 43\cdot 191\cdot 1201\cdot 2801$
$\mathbb{F}_{53}$	$2^2\cdot 3^3\cdot 13\cdot 53$	$2^5\cdot 3^3\cdot 7\cdot 13^2\cdot 53^3\cdot 409$	$2^7\cdot 3^6\cdot 5\cdot 7\cdot 13^3\cdot 53^6\cdot 281\cdot 409$	$2^{11}\cdot 3^6\cdot 5\cdot 7\cdot 11\cdot 13^4\cdot 53^{10}\cdot 131\cdot 281\cdot 409\cdot 5581$
$\mathbb{F}_{59}$	$2^2\cdot 3\cdot 5\cdot 29\cdot 59$	$2^4\cdot 3\cdot 5\cdot 29^2\cdot 59^3\cdot 3541$	$2^7\cdot 3^2\cdot 5^2\cdot 29^3\cdot 59^6\cdot 1741\cdot 3541$	$2^9\cdot 3^2\cdot 5^2\cdot 11\cdot 29^4\cdot 41\cdot 59^{10}\cdot 151\cdot 181\cdot 1741\cdot 3541$

Fin du cours 12

5. Groupes orthogonaux euclidiens

On munit $\mathbb{R}^n$ du produit scalaire canonique $(\cdot|\cdot)$. On note $\|\cdot\|$ la norme associée. Pour tout sous-espace vectoriel, on note $V^\perp = \{x \in \mathbb{R}^n \,|\, \forall v \in V, (x|v) = 0\}$. On rappelle que l'on a pour tout V :

$$V \oplus V^\perp = \mathbb{R}^n$$

Le *groupe orthogonal euclidien* est le sous-groupe de $\mathrm{GL}_n(\mathbb{R})$ des isométries euclidiennes donné par :

$$\begin{aligned} \mathrm{O}_n(\mathbb{R}) &= \{g \in \mathrm{GL}_n(\mathbb{R}) \,|\, g^T g = 1\} \\ &= \{g \in \mathrm{GL}_n(\mathbb{R}) \,|\, g g^T = 1\} \\ &= \{g \in \mathrm{GL}_n(\mathbb{R}) \,|\, \forall x \in \mathbb{R}^n, \|gx\| = \|x\|\} \\ &= \{g \in \mathrm{GL}_n(\mathbb{R}) \,|\, \forall x, y \in \mathbb{R}^n, (gx|gy) = (x|y)\} \end{aligned}$$

et on note $\mathrm{SO}_n(\mathbb{R})$ le sous-groupe de $\mathrm{O}_n(\mathbb{R})$ des applications qui préservent l'orientation, égale celle de déterminant positif, égale celle de déterminant 1. On l'appelle le *groupe spécial orthogonal eucilidien*. On oublie souvent le mot euclidien dans ses dénominations.

I Générateurs

Une *réflexion* (euclidienne) est une isométrie (euclidienne) g tel que $\dim\ker(g-1) = n-1$. Si H est un hyperplan, la réflexion σ_H d'hyperplan H est la réflexion tel que $\ker(\sigma_H - 1) = H$. Dans une b.o.n., la matrice de σ_H est :

$$\begin{pmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}.$$

Si v est un vecteur de norme 1 qui dirige $H^\perp$ alors :

$$\sigma_H(x) = x - (x|v)v$$

Un *retournement* est une isométrie (euclidienne) g tel que $\dim\ker(g-1) = n-2$ et $\dim\ker(g+1) = 2$. Dans une b.o.n., la matrice de g est :

$$\begin{pmatrix} -1 & & & & \\ & -1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}.$$

Si Π est un plan, le retournement τ_Π de plan Π est le retournement tel que $\ker(\tau_\Pi+1) = \Pi$ et $\ker(\tau_\Pi - 1) = \Pi^\perp$.

Proposition I.1 Le groupe $\mathrm{O}_n(\mathbb{R})$ est engendré par les réflexions.

Démonstration. La proposition est vraie pour $n = 1$. Soit $n \geqslant 2$. On suppose que la proposition est vraie en dimension $n-1$. Soit g quelconque et v vecteur non nul. Si $g(v) = v$ alors $g(v^\perp) = v^\perp$ or $\dim(v^\perp) = n-1$. Ainsi g restreint à $v^\perp$ est un produit de réflexions de $v^\perp$ que l'on peut prolonger par l'identité à $\mathbb{R}^n$ pour obtenir que g est un produit de réflexions par le premier paragraphe.

Sinon $g(v) \neq v$. Il existe une réflexion σ tel que $\sigma(v) = g(v)$. Ainsi, σg fixe v donc est un produit de réflexions, d'où le résultat. ∎

Proposition I.2 Pour $n \geqslant 3$. Le groupe $\mathrm{SO}_n(\mathbb{R})$ est engendré par les retournements.

Démonstration. Tout isométrie de $\mathrm{SO}_n(\mathbb{R})$ est produit d'un nombre pair de réflexions. Il suffit donc de montrer que tout produit $\sigma_1\sigma_2$ de réflexions est égale à un produit de deux retournements.

On fait d'abord le cas $n = 3$. La forme matricielle nous montre que si σ est une réflexion alors $-\sigma$ est un retournement, on a donc : $\sigma_1\sigma_2 = (-\sigma_1)(-\sigma_2)$.

Soient σ_1, σ_2 deux réflexions d'hyperplans H_1 et H_2. On choisit V un sous-espace de codimension 3 inclus dans $H_1 \cap H_2$. Ainsi $V^\perp$ est préservé par σ_1 et σ_2 et de dimension 3 ainsi on note τ_i l'isométrie $-\sigma_i$ sur $V^\perp$ et l'identité sur V. Ainsi, les τ_i sont des retournements et $\sigma_1\sigma_2 = \tau_1\tau_2$. D'où le résultat. ∎

II Action transitive et conséquences : conjugaison, centre

Proposition II.1 Le groupe $\mathrm{SO}_n(\mathbb{R})$ agit simplement transitivement sur les b.o.n.d.

Démonstration. Par définition, une matrice est dans $\mathrm{SO}_n(\mathbb{R})$ si et seulement si la famille de ses vecteurs colonnes forment une b.o.n.d. ∎

Proposition II.2 Le groupe $\mathrm{SO}_n(\mathbb{R})$ agit transitivement sur les espaces de dimension k.

Démonstration. Toute base s'orthonormalise par le procédé de Gramm-Schmidt d'où le résultat via le point précédent. ∎

Proposition II.3 — Principe de conjugaison.

$$\forall g \in \mathrm{O}_n(\mathbb{R}), \quad g\sigma_H g^{-1} = \sigma_{g(H)} \quad \text{et} \quad g\tau_\Pi g^{-1} = \tau_{g(\Pi)}$$

Démonstration. Exo. ■

Corollaire II.4 Les réflexions sont conjugués dans $\mathrm{O}_n(\mathbb{R})$, les retournements sont conjugués dans $\mathrm{SO}_n(\mathbb{R})$

Démonstration. Le groupe $\mathrm{SO}_n(\mathbb{R})$ agit transitivement sur les hyperplans et sur les plans. ■

Proposition II.5 Les centres sont :

	n=2	n pair	n impair
$\mathrm{O}_n(\mathbb{R})$	$\{\pm 1\}$	$\{\pm 1\}$	$\{\pm 1\}$
$\mathrm{SO}_n(\mathbb{R})$	$\mathrm{SO}_2(\mathbb{R})$	$\{\pm 1\}$	$\{1\}$

Démonstration. On laisse le cas $n = 2$ en exo. On suppose $n \geqslant 3$. Soit $g \in \mathrm{O}_n(\mathbb{R})$ qui centralise $\mathrm{SO}_n(\mathbb{R})$. En particulier, g commute à tous les retournements donc $g(\Pi) = \Pi$ pour tous les plans. Donc, $g(D) = D$ pour tous les droites (car $n \geqslant 3$), donc g est une homothétie or g est une isométrie donc $g = \pm Id$... ■

III Topologie

Proposition III.1 Le groupe $\mathrm{SO}_n(\mathbb{R})$ est connexe et compacte.

Démonstration. On commence par montrer que $\mathrm{O}_n(\mathbb{R})$ est compacte. En effet $g \in \mathrm{O}_n(\mathbb{R})$ signifie que $g^T g = 1$, par suite :

$$\mathrm{O}_n(\mathbb{R}) \quad \text{est fermé et} \quad \forall j, \quad \sum_i g_{ij}^2 = 1 \quad \text{donc } \mathrm{O}_n(\mathbb{R}) \text{ est borné.}$$

Tout élément de $\mathrm{SO}_n(\mathbb{R})$ est somme de rotations dans des plans (voir TD), i.e :

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & R_{\theta_1} & & \\ & & & & \ddots & \\ & & & & & R_{\theta_r} \end{pmatrix}$$

On ramène tous les angles à zéro. Donc $\mathrm{SO}_n(\mathbb{R})$ est connexe par arcs, donc connexe. ■

IV Simplicité

Proposition IV.1 Si $n \neq 1, 2, 4$ alors le groupe $\mathrm{PSO}_n(\mathbb{R})$ est simple. Autrement dit,

- Le groupe $\mathrm{SO}_n(\mathbb{R})$ est simple pour $n \geqslant 3$ impair.
- Le groupe ${}^{\mathrm{SO}_n(\mathbb{R})}/_{\{\pm 1\}}$ est simple pour $n \geqslant 6$ pair.

Démo pour $\mathrm{SO}_3(\mathbb{R})$. Soit $N \lhd \mathrm{SO}_3(\mathbb{R})$. On va montrer que N contient un retournement ou est central. Soit $n \in N$. On considère :

$$\begin{array}{rccc} \varphi_n : & \mathrm{SO}_3(\mathbb{R}) & \to & [0,\pi] \\ & g & \mapsto & \arccos((\mathrm{Tr}([g,n])-1)/2) = \theta([g,n]) \end{array}$$

L'application φ_n est continue et le groupe $\mathrm{SO}_3(\mathbb{R})$ est compact et connexe donc $\mathrm{Im}(\varphi_n)$ est un segment $I_n = [0,a_n]$. On a deux cas à distinguer.

- Cas 1 : $\forall n \in N$, on a $I_n = \{0\}$.
- Cas 2 : $\exists \varepsilon > 0$, $\exists n \in N$, tel que $I_n \supset [0,\varepsilon]$.

On commence par remarquer $\theta([g,n]) = 0 \Leftrightarrow [g,n] = 1$. Autrement dit, le cas 1 entraine que $N \leqslant Z = \{1\}$. Ce qui conclut le cas 1.

On suppose à présent que l'on est dans le cas 2. Ils existent donc un entier $k \in \mathbb{N}$, $n \in N$ et $g \in \mathrm{SO}_3(\mathbb{R})$ tel que $[g,n] \in N$ est une rotation d'angle π/k. Par suite, $[g,n]^k$ est une rotation d'angle π. Autrement dit, un retournement. Or les retournements sont conjugués et N est distingué donc N contient tous les retournements. Or les retournements engendrent $\mathrm{SO}_3(\mathbb{R})$ donc $N = \mathrm{SO}_3(\mathbb{R})$. ■

V Décompositions dans les groupes linéaires réels et complexes

On va définir quelques notations :

G	K	P	A	A^+	N
$\mathrm{GL}_n(\mathbb{R})$	$\mathrm{O}_n(\mathbb{R})$	$\mathrm{Sym}_n^{++}(\mathbb{R})$	$\mathrm{Diag}_+(\mathbb{R})$		$\mathrm{UniTri}_n(\mathbb{R})$
$\mathrm{SL}_n(\mathbb{R})$	$\mathrm{SO}_n(\mathbb{R})$	$\mathrm{SSym}_n^{++}(\mathbb{R})$	$\mathrm{SDiag}_+(\mathbb{R})$		$\mathrm{UniTri}_n(\mathbb{R})$
$\mathrm{GL}_n(\mathbb{C})$	U_n	Herm_n^{++}	$\mathrm{Diag}_+(\mathbb{R})$		$\mathrm{UniTri}_n(\mathbb{C})$
$\mathrm{SL}_n(\mathbb{C})$	SU_n	SHerm_n^{++}	$\mathrm{SDiag}_+(\mathbb{R})$		$\mathrm{UniTri}_n(\mathbb{C})$

où

1. Sym (resp. Herm) signifie les matrices symétriques (resp. hermitiennes).
2. L'ajout d'un ++ signifie définie positive (le résultat est un cône convexe stable par $g \mapsto g^{-1}$).
3. L'ajout d'un S signifie de déterminant 1.
4. La lettre O (resp. U) signifie orthogonal (resp. unitaire).
5. Les abréviations Diag (resp. UniTri) signifie matrices diagonales (resp. unitriangulaires).
6. La notation $X(k)$ signifie que les coefficients sont dans k.
7. A^+ est le sous-ensemble fermé de A tels que les valeurs propres sont rangées par ordre décroissant ou encore A^+ est l'ensemble des matrices diagonales, à diagonale strictement positive tels que $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_n$.

On remarquera que K, A, N sont des groupes tandis que P, A^+ ne sont pas des groupes.

1. Décomposition polaire

Théorème V.1 — Décomposition polaire. L'application :

$$\begin{array}{rccc} \varphi : & \mathrm{O}_n(\mathbb{R}) \times \mathrm{Sym}_n^{++} & \to & \mathrm{GL}_n(\mathbb{R}) \\ & (Q,S) & \mapsto & QS \end{array}$$

est un homéomorphisme.

R

- On peut changer $(Q,S) \mapsto QS$ en $(Q,S) \mapsto SQ$, l'énoncé et la preuve sont encore valides.
- On peut changer $\mathrm{U}_n(\mathbb{C}) \times H_n^{++} \to \mathrm{GL}_n(\mathbb{C})$, $K = \mathrm{U}_n(\mathbb{C})$ est le groupe unitaire, $P = H_n^{++}$ est le cône des matrices hermitiennes définies positives.
- On peut changer $\mathrm{GL}_n(\mathbb{R})$ en $\mathrm{SL}_n(\mathbb{R})$, si on change $\mathrm{O}_n(R)$ en $\mathrm{SO}_n(R)$ et S_n^{++} en les définies positives de déterminant 1.
- Idem sur $\mathbb{C}$.
- Autrement dit, on a $K \times P \xrightarrow{\sim} G$ via $(Q,S) \mapsto QS$.

R Le nom vient de l'énoncé en dimension 1 sur $\mathbb{C}$ puisqu'il devient :

$$\begin{array}{rccc} \varphi : & \mathbb{S}^1 \times \mathbb{R}_*^+ & \longrightarrow & \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times \\ & (e^{i\theta}, r) & \mapsto & e^{i\theta} r \end{array}$$

Corollaire V.2 Le groupe $\mathrm{GL}_n(\mathbb{R})$ est homéomorphe à $\mathrm{O}_n(\mathbb{R}) \times \mathbb{R}^{n(n+1)/2}$.

Démonstration. L'espace S_n^{++} est un cône convexe ouvert de S_n qui est un espace vectoriel de dimension $n(n+1)/2$. ∎

Lemma V.3 L'application $M \mapsto M^2$ restreinte à S_n^{++} est un homéo. On note $\sqrt{\cdot}$ sa réciproque.

Démonstration. L'application est $M \mapsto M^2$ est clairement continue et bijective (exo TD). Il suffit donc de montrer que si M_n^2 converge vers N_∞ alors M_n converge. On diagonalise M_n, ils existent $k_n \in K$ et a_n diagonale, à diagonale strictement positive, tels que :

$$M_n = k_n a_n k_n^{-1}$$

- La suite $(a_n^2)_n$ converge or la suite $(a_n)_n$ est strictement positive donc la suite $(a_n)_n$ converge donc incluse dans un compact de $\mathrm{GL}_n(\mathbb{R})$.
- La suite $(k_n)_n$ est incluse dans un compact donc la suite $(M_n)_n$ est aussi incluse dans un compact de $\mathrm{GL}_n(\mathbb{R})$..
- Toute valeur d'ahérence de la suite $(M_n)_n$ est une racine carré de N_∞ donc la suite $(M_n)_n$ possède une unique valeur d'adhérence.
- *Rappel :* Si une suite à valeurs dans un compact n'a qu'une valeur d'ahérence alors cette suite converge.

Donc $(M_n)_n$ converge vers $\sqrt{N_\infty}$. ∎

Démonstration. On remarque l'implication suivante :

$$g = QS \quad \Rightarrow g^T g = (QS)^T QS = S^T S = S^2$$

La matrice $g^T g$ est définie positive. On peut et on doit prendre $S = \sqrt{g^T g}$. On pose : $Q = gS^{-1}$. Vérifions que $Q^T Q = 1$.

$$Q^T Q = (gS^{-1})^T gS^{-1} = S^{-1} g^T gS^{-1} = S^{-1} S^2 S^{-1} = 1$$

L'application φ est donc bijective. On remarque qu'elle est continue.

Reste à montrer que sa réciproque est continue. On vient d'obtenur des formules pour cette réciproque :

$$S = \sqrt{g^T g} \quad Q = gS^{-1}$$

Donc la réciproque est continue. ■

2. Décomposition de Cartan

Théorème V.4 — Décomposition de Cartan ou SVD.
Soit $G = \mathrm{GL}_n(\mathbb{R}), \mathrm{SL}_n(\mathbb{R}), \mathrm{GL}_n(\mathbb{C}), \mathrm{SL}_n(\mathbb{C})$. L'application $K \times A^+ \times K \to G$ donnée par $(k,a,l) \mapsto kal$ est surjective. Le facteur $a \in A^+$ étant unique. Les facteurs $k,l \in K$ sont "presque" uniques si les valeurs propres de a sont toutes distinctes.

R Les réels de la diagonale de a sont les valeurs propres ordonnées de $g^T g$, on les appelle les *valeurs singulières* de g.

Démo pour $G = \mathrm{GL}_n(\mathbb{R})$. *Existence :* On reprend les notations précédentes $M = QS$. Puisque S est symétrique on peut la diagonaliser dans une base orthonormée, comme elle est définie positive ses valeurs propres seront strictement positives. Ils existent donc un $R \in K$ et un unique $a \in A^+$ tel que :

$$S = RaR^{-1} = RaR^T \qquad \text{et donc} \qquad g = QS = (QR)aR^T$$

Unicité : Si $g = kal$ alors $kl(l^T al)$ est la décomposition polaire de g puisque $(l^T al)$ est définie positive donc $l^T al$ est la **diagonalisation ordonnée** de $g^T g$ donc a est unique quoi qu'ils arrivent. Si les valeurs propres de a sont toutes distinctes. Les colonnes de l^T sont données par les vecteurs propres ordonnées de $g^T g$, ils sont donc uniques au signe près. Autrement dit, $l' = \varepsilon l \varepsilon$ où ε est une matrice diagonale avec des 1 ou des -1. Donc l est presque unique et donc k est presque unique. ■

3. Décomposition d'Iwasawa

Théorème V.5 — Décomposition d'Iwasawa ou QR.
Soit $G = \mathrm{GL}_n(\mathbb{R}), \mathrm{SL}_n(\mathbb{R}), \mathrm{GL}_n(\mathbb{C}), \mathrm{SL}_n(\mathbb{C})$. L'application $K \times A \times N \to G$ est un homéomorphisme.

Démonstration. Voir TD. *Ind. Appliquer Gram-Schmidt à g : Il existe $k \in K$ et $u \in AN$ tel que $k = gu$...* ■

VI Sous-groupe compact des groupes linéaires réels et complexes

Théorème VI.1 Soit $G = \mathrm{GL}_n(\mathbb{R}), \mathrm{SL}_n(\mathbb{R}), \mathrm{GL}_n(\mathbb{C}), \mathrm{SL}_n(\mathbb{C})$. Soit L un sous-groupe compact de G, il existe $g \in G$ tel que $gLg^{-1} \leqslant K$. Autrement dit, K est le sous-groupe compact maximal de G.

Démonstration. On fait agir G sur les matrices symétriques définies positives via :

$$g \cdot S = gSg^T$$

On cherche une matrice S_L tel que :

$$\forall g \in L, \quad g \cdot S_L = S_L$$

Cela signifiera que, le produit scalaire :

$$\langle X|Y\rangle = X^T S_L Y$$

est préservé par L, ou encore que $\sqrt{S}L\sqrt{S}^{-1} \leqslant K$.

Soit S_0 une matrice symétrique définie positive quelconque. Il est important de remarquer l'espace des matrices symétriques définies positives est un cône convexe de l'espace des matrices symétriques. L'orbite $L \cdot S_0$ est un compact de ce cône, donc l'enveloppe convexe $\mathcal{C}$ est aussi compacte [1], le barycentre S_L de $\mathcal{C}$ est une matrice définie positive invariante par L.

Si L est un groupe fini, on peut-être explicite :

$$S_L = \frac{1}{\#L} \sum_{g \in L} g \cdot S_0$$

■

VII Sous-groupe fermé des groupes linéaires réels et complexes

Théorème VII.1 — Théorème de Cartan - von Neumann. Tout sous-groupe fermé de $\mathrm{GL}_n(\mathbb{R})$ ou $\mathrm{GL}_n(\mathbb{C})$ est une sous-variété.

VIII Géométrie sphérique

1. Théorème de Girard

On note $\mathbb{S}^2$ la sphère unitée de $\mathbb{R}^3$. On l'appelle la sphère de dimension 2.

1. Un *grand cercle* est l'intersection d'un plan vectoriel avec la sphère $\mathbb{S}^2$. Une *géodésique*/*segment* est un arc de grand cercle.
2. Deux points x, y sur la sphère sont dit antipodaux si $y = -x$.
3. La distance entre deux points $x, y \in \mathbb{S}^2$ est :

$$\mathrm{dist}_{\mathbb{S}^2}(x,y) = d(x,y) = \theta = 2\arcsin\left(\mathrm{dist}_{\mathbb{R}^3}(x,y)/2\right)$$

4. On remarquera qu'entre deux points non antipodaux, il existe une unique géodésique et que la longueur (comme courbe de $\mathbb{R}^3$, i.e. longueur = intégrale de la vitesse) de celle-ci est la distance entre les deux points.
5. L'angle (non-orienté) entre deux grands cercles $\Pi_1 \cap \mathbb{S}^2$ et $\Pi_2 \cap \mathbb{S}^2$ est l'angle entre les droites $\Pi_1 \cap (\Pi_1 \cap \Pi_2)^\perp$ et $\Pi_2 \cap (\Pi_1 \cap \Pi_2)^\perp$.

1. Théorème de Carathéodory : env. convexe d'un compact est compact en dimension finie.

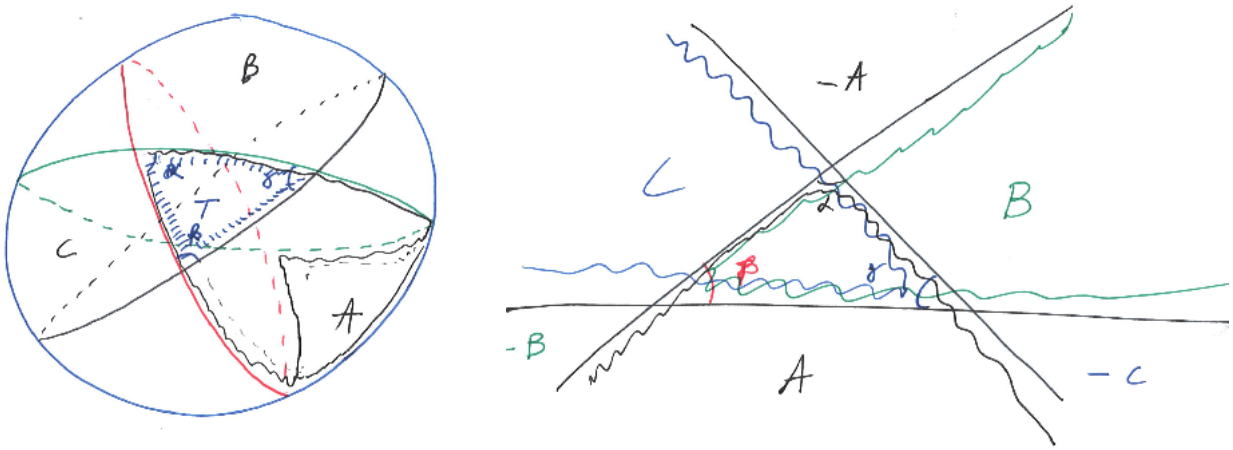

FIGURE 5.1 – Le beau dessin

6. Il existe une unique mesure λ $O_3(\mathbb{R})$-invariante sur la sphère telle que $\lambda(\mathbb{S}^2) = 4\pi$. L'existence est donnée par prendre $\lambda(\mathcal{A}) = 3\text{Leb}(\text{cône}(\mathcal{A}) \cap \mathbb{B}^2)$. L'unicité est donnée par reconstruire la mesure de Lebesgue via une telle mesure λ. On n'en aura pas besoin donc on ne fait pas.
7. La lune A d'angle α vérifie $\lambda(A) = 2\alpha$.

Théorème VIII.1 — Girard. L'aire d'un triangle d'angles α, β, γ sur la sphère vérifie :

$$\mathcal{A} = \alpha + \beta + \gamma - \pi$$

Démonstration. Bien dire qu'on s'en fout des bords des A, B, C. On fait un beau dessin, on remarque la sphère est l'union $(A \cup B \cup C)$ et $-(A \cup B \cup C)$; mais $A \cap (-B \cup -C)$ est vide. L'union précédente est donc une partition. De plus, $A \cap B = B \cap C = C \cap A = T$, d'où :

$$\begin{array}{rcl} \text{Aire}(\frac{1}{2}\mathbb{S}^2) & = & A + B + C - 3T + T \\ 2\pi & = & 2\alpha + 2\beta + 2\gamma - 2\mathcal{A} \end{array}$$

■

Corollaire VIII.2 En géométrie sphérique, la somme des angles d'un triangle est strictement plus grande que π.

Corollaire VIII.3 Si P est un polygone d'angles $\alpha_1, \cdots, \alpha_n$ alors :

$$\mathcal{A} = \sum \alpha_i - (n-2)\pi$$

2. Théorème d'Euler

Corollaire VIII.4 — Euler. Si P est un polyèdre convexe alors $S - A + F = 2$.

Démonstration. On met notre polyèdre dans la sphère $\mathbb{S}^2$, on a :

$$\begin{aligned}
\text{Aire}(\mathbb{S}^2) &= \sum_{f \text{ faces}} \text{Aire}(f) \\
4\pi &= \sum_{f \text{ faces}} \left(\sum_{s,\text{sommets de } f} \alpha_s(f) - (\text{nb aretes de } f - 2)\pi \right) \\
4\pi &= \sum_{f \text{ faces}} \left(\sum_{s,\text{sommets de } f} \alpha_s(f) \right) - \pi \sum_{f \text{ faces}} (\text{nb aretes de } f) + 2\pi F \\
4\pi &= 2\pi S - \pi 2A + 2F\pi
\end{aligned}$$

■

3. Théorème de Platon

Un *polytope* est l'enveloppe convexe d'un nombre fini de points de $\mathbb{R}^n$ non-inclus dans un hyperplan. Si $n = 2$ alors on parle de *polygone*, si $n = 3$, on parle de *polyèdre*.

Un drapeau d'un polytope est une suite $f_0 \subset f_1 \subset \cdots \subset f_{n-1}$ où f_i est une face de dimension i du polytope.

Le groupe d'isométries d'un polytope P est le sous-groupe de $\text{Isom}(\mathbb{R}^n)$ qui préserve le sous-ensemble P de $\mathbb{R}^n$.

Un polytope est dit *régulier* si son groupe d'isométries agit transitivement sur ces drapeaux (sommet dans arête dans face). En particulier, dans un tel polyèdre toutes les faces ont le même nombres de côtés et tous les sommets ont le même nombre de voisins.

Théorème VIII.5 Pour tout $n \geqslant 3$, il existe un unique polygone régulier à n côtés. Son groupe d'isométrie est le groupe diédral d'ordre $2n$.

Théorème VIII.6 — Platon, ≃ -400. Il n'existe que 5 polyèdres réguliers.

Théorème VIII.7 — Schläfli, 1850. Il existe 6 4-polytopes réguliers et pour tout $n \geqslant 5$, il existe 3 polytopes réguliers.

Démonstration. On note v la valence de tout sommet de P, et n le nombre de côtés de toutes les faces. On a : $Sv = 2A$ en comptant les sommets dans arêtes, et $2A = nF$ en comptant les arêtes dans faces. On en tire : $S = \frac{2A}{v}$ et $F = \frac{2A}{n}$, d'où :

$$\frac{1}{v} + \frac{1}{n} = \frac{1}{A} + \frac{1}{2}$$

On se rappelle que $A > 0, n, v \geqslant 3$, on mouline, on obtient : $(v,n) = (3,3),(3,4),(4,3),(3,5),(5,3)$, ce qui permet de calculer S, A, F pour chaque cas. Ce qui montre qu'il y a au plus 5 polyèdres réguliers, après il faut les construire pour vérifier qu'ils existent bien... ■

	S	A	F	n	v	$\text{Isom}(P)$	$\text{Isom}^+(P)$
Tétraèdre	4	6	4	3	3	$\mathfrak{S}_4$	$\mathfrak{A}_4$
Cube	8	6	6	4	3	$\mathfrak{S}_4 \times \{\pm\text{Id}\}$	$\mathfrak{S}_4$
Octaèdre	6	6	8	3	4	$\mathfrak{S}_4 \times \{\pm\text{Id}\}$	$\mathfrak{S}_4$
Dodécaèdre	20	30	12	5	3	$\mathfrak{A}_5 \times \{\pm\text{Id}\}$	$\mathfrak{A}_5$
Icosaèdre	12	30	30	3	5	$\mathfrak{A}_5 \times \{\pm\text{Id}\}$	$\mathfrak{A}_5$

En dimension $n \geqslant 4$, on a le n-simplexe ($\mathrm{Isom}^+ = \mathfrak{S}_n$), le n-cube et son dual ($\mathrm{Isom}^+ = \mathfrak{S}_n \times \{\pm \mathrm{Id}\}$). En dimension 4, il y a 3 exceptionnels en plus, le 120-cell fait de 120 dodécaèdres, dont le groupe d'isométries est un groupe nommé H_4 d'ordre 14 400, son dual est aussi un polyèdre régulier : le 600-cell. Enfin, il reste le dernier qui est auto-dual : le 24-cell fait de 24 octaèdres, son groupe d'isométries est F_4 d'ordre 1152...

IX Sous-groupes finis des groupes orthogonaux de petite dimension

Proposition IX.1 Tout sous-groupe fini de $\mathrm{SO}_2(\mathbb{R})$ est cyclique. Inversement, tout groupe cyclique se réalise comme un sous-groupe de $\mathrm{SO}_2(\mathbb{R})$.

Tout sous-groupe de $\mathrm{O}_2(\mathbb{R})$ non-inclus dans $\mathrm{SO}_2(\mathbb{R})$ est diédral. Tous les groupes diédraux d'ordre $2n$ pour $n \geqslant 1$ se réalise comme sous-groupe de $\mathrm{O}_2(\mathbb{R})$ non-inclus dans $\mathrm{SO}_2(\mathbb{R})$, comme groupe de symétrie d'un polygone régulier à n côtés.

Tout sous-groupe de $\mathrm{SO}_3(\mathbb{R})$ est cyclique, diédral ou isomorphe à $\mathfrak{A}_4$, $\mathfrak{A}_4 \times \mathbb{Z}_{/2\mathbb{Z}}$ ou $\mathfrak{A}_5$. Tous les cas se réalisent, les 3 derniers via les groupes de symétries des 5 polyèdres réguliers.

X Les quaternions

1. Une première définition

On note $\mathcal{H}$ la $\mathbb{R}$-algèbre $\mathcal{H} = \mathbb{R}1 \oplus \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ où on impose les lois :

$$i^2 = j^2 = k^2 = -1 \quad ij = k \quad jk = i \quad ki = j$$

La vérification de l'associativité de la multiplication est pénible...

Si $x = a + bi + cj + dk$ alors on note $\bar{x} = a - bi - cj - dk$. Un calcul montre que :

$$x\bar{x} = |x|^2$$

Il est clair que 1 est central dans $\mathcal{H}$. On obtient donc que $\mathcal{H}$ est une algèbre à division.

2. Une deuxième définition

On note $\mathbb{H}$ la sous-algèbre de $\mathrm{M}_2(\mathbb{C})$ définie par :

$$\mathbb{H} = \left\{ \begin{pmatrix} w & -z \\ \bar{z} & \bar{w} \end{pmatrix} \quad | \quad w, z \in \mathbb{C} \right\}$$

Proposition X.1 Le $\mathbb{R}$-s.e.v $\mathbb{H}$ est une sous-algèbre de la $\mathbb{R}$-algèbre $\mathrm{M}_2(\mathbb{C})$.

Démonstration. Il suffit de montrer que $\mathbb{H}$ est stable par produit. L'associativité est offerte. ∎

Si on pose :

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad k = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

Alors l'application induite de $\varphi : \mathbb{H} \to \mathcal{H}$ est un isomorphisme, on a :

$$a + ib + jc + kd = \begin{pmatrix} a+ib & -(c+id) \\ c-id & a-ib \end{pmatrix} \quad \text{et} \quad \overline{a + ib + jc + kd} = \overline{\begin{pmatrix} a+ib & -(c+id) \\ c-id & a-ib \end{pmatrix}}^T$$

R On a :

$$\mathrm{Com}^T\begin{pmatrix} w & -z \\ \bar{z} & \bar{w} \end{pmatrix} = \begin{pmatrix} \bar{w} & z \\ -\bar{z} & w \end{pmatrix} = \overline{\begin{pmatrix} w & -z \\ \bar{z} & \bar{w} \end{pmatrix}}^T$$

On retrouve ainsi la formule :

$$x\bar{x} = |x|^2 \quad \text{et on gagne sans calcul la formule :} \quad \overline{xy} = \bar{x}\bar{y} \quad \text{et} \quad |xy|^2 = |x|^2|y|^2$$

R Le *théorème des 4 carrés* affirme que tout entier est somme de 4 carrés. La démonstration est en deux étapes.

- Étape astucieuse mais facile : le produit d'une somme de 4 carrés est une somme de 4 carrés (c'est une conséquence de $|x|^2|y|^2 = |xy|^2$).
- Deuxième étape arithmétique et difficile. Tout nombre premier est somme de 4 carrés.

R On peut munir $\mathbb{S}^3 = \mathbb{S}(\mathbb{H})$ d'une structure de groupe, tout comme $\mathbb{S}^0 = \mathbb{S}(\mathbb{R})$ et $\mathbb{S}^1 = \mathbb{S}(\mathbb{C})$ est muni d'une loi de groupe. Cette loi est continue, la multiplication et le passage à l'inverse sont des applications continues.

Théorème X.1 Soit $n \geqslant 0$, si la sphère $\mathbb{S}^n$ peut-être muni d'une loi de groupe alors $n \in \{0,1,3\}$.

3. Lien avec le groupe SU_2

Proposition X.2 En coordonnées $\mathbb{H} \leqslant \mathrm{M}_2(\mathbb{C})$, on a l'égalité :

$$\mathbb{S}(\mathbb{H}) = \mathrm{SU}_2$$

Démonstration. On commence par remarquer que SU_2 et $\mathbb{H}$ sont des sous-ensembles de $\mathrm{M}_2(\mathbb{C})$. Ensuite, SU_2 et $\mathbb{S}(\mathbb{H})$ sont des sous-ensembles de $\mathrm{SL}_2(\mathbb{C})$. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$,

$$M \in \mathrm{SU}_2 \Leftrightarrow \begin{cases} M^{-1} = \bar{M}^T \\ \det(M) = 1 \end{cases} \Leftrightarrow \begin{cases} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} \\ \det(M) = 1 \end{cases} \Leftrightarrow M \in \mathbb{S}(\mathbb{H})$$

■

4. Le centre de $\mathbb{H}$

Proposition X.3 Le centre de $\mathbb{H}$ est $\mathrm{Re}\mathbb{H} = \mathbb{R}1$.

Démonstration. L'inclusion $\mathbb{R}1 \subset \mathrm{Re}\mathbb{H}$ est claire. Si $x = a + ib + cj + dk$ commutte avec i alors :

$$(a+ib+cj+dk)i = -b + ai + dj - ck = i(a+ib+cj+dk) = -b + ai - dj + ck$$

Donc $d = c = 0$. On recommence avec k ou j, on obtient $b = c = d = 0$. ■

5. Lien avec le groupe $\mathrm{SO}_4(\mathbb{R})$

On définit une action de $\mathbb{S}(\mathbb{H})\times\mathbb{S}(\mathbb{H})$ sur $\mathbb{H}$ via $(u,v)\cdot x = uxv^{-1}$, cette action est linéaire, préserve la norme, elle fournit donc un morphisme continue :

$$\mathbb{S}(\mathbb{H})\times\mathbb{S}(\mathbb{H}) \to \mathrm{O}(\mathbb{H},\det) \simeq \mathrm{O}_4(\mathbb{R})$$

Or, $\mathbb{S}(\mathbb{H})\times\mathbb{S}(\mathbb{H})$ est connexe donc on a en fait un morphisme continue :

$$\mathbb{S}(\mathbb{H})\times\mathbb{S}(\mathbb{H}) \to \mathrm{SO}(\mathbb{H},\det) \simeq \mathrm{SO}_4(\mathbb{R})$$

Théorème X.4 Ce morphisme est surjectif et son noyau est le groupe :

$$\{(1,1),(-1,-1)\}$$

Démonstration. On commence par le noyau. Si (u,v) est dans le noyau alors :

$$u1v^{-1} = v \quad \text{donc} \quad u = v$$

Ensuite, on a aussi :

$$uiu^{-1} = u \quad \text{donc} \quad ui = iu$$

De même, on a :

$$uj = ju \quad \text{et} \quad uk = ku$$

Donc $u \in Z(\mathbb{H}) \cap \mathbb{S}(\mathbb{H}) = \{\pm 1\}$.

On a la formule suivante :

$$x,y \in \mathbb{H}, \quad y\bar{x}y = 2(x|y) - (y|y)x$$

On définit :

$$\text{Pour } u \in \mathbb{S}(\mathbb{H}), \quad \sigma(u) = -u\bar{x}u$$

On vérifie sans peine que σ_u est la réflexion orthogonale d'hyperplan $u^\perp$. Toute isométrie directe est produit d'un nombre paire de réflexions, il nous suffit donc de montrer que tout produit de deux réflexions est dans l'image de $\mathbb{S}(\mathbb{H})\times\mathbb{S}(\mathbb{H})$.

$$\sigma_u(\sigma_v(x)) = u\overline{v\bar{x}\bar{v}}u = u\bar{v}x\bar{v}u$$

D'où le résultat. ∎

6. Lien avec le groupe $\mathrm{SO}_3(\mathbb{R})$

On définit une action de $\mathbb{S}(\mathbb{H})$ sur $\mathbb{H}$ via $u\cdot x = uxu^{-1}$. Cette action est linéaire et préserve la norme et le sous-espace $\mathrm{Re}\mathbb{H} = \mathbb{R}1$, elle fournit donc un morphisme continue :

$$\mathbb{S}(\mathbb{H}) \to \mathrm{O}(\mathrm{Im}\mathbb{H}) \simeq \mathrm{O}_3(\mathbb{R})$$

Or $\mathbb{S}(\mathbb{H})$ est connexe donc on a en fait un morphisme continue :

$$\mathbb{S}(\mathbb{H}) \to \mathrm{SO}(\mathrm{Im}\mathbb{H}) \simeq \mathrm{SO}_3(\mathbb{R})$$

Théorème X.5 Ce morphisme est surjectif de noyau $\{\pm 1\}$.

Démonstration. Si u est dans le noyau alors u est central donc $u = \pm 1$. Soit $g \in \mathrm{SO}(\mathrm{Im}(\mathbb{H}))$, on prolonge g à $\mathbb{H}$ par l'identité, on obtient un élément de $\mathrm{SO}(\mathbb{H})$ qui fixe 1. Par le théorème précédent, il est de la forme $x \mapsto uxv^{-1}$, mais il fixe 1 donc $u = v$. ■