LISTES DE DÉVELOPPEMENTS POSSIBLES EN ALGÈBRE POUR L'AGRÉGATION

ÉTIENNE MANN

Sommaire

1. Simplicité de $PSL(n,k)$ 2
2. Simplicité de $O^+(3,\mathbb{R})$ 2
3. Simplicité de $PO^+(n,\mathbb{R})$ pour $n \geq 5$ 3
4. Classes d'équivalence dans $M_{n\times p}(A)$ et deux applications 3
5. Réduction de Frobenius et réduction de Jordan par les $\mathbb{K}[X]$-module 4
6. Théorèmes de Sylow 6
7. Décomposition polaire de $GL(n,\mathbb{R})$ 6
8. Théorème des zéros de Hilbert 7
9. Sous groupes finis de $O(2,\mathbb{R})$ et de $O(3,\mathbb{R})$ 7
10. Loi de réciprocité quadratique par le lemme chinois 8
11. Le groupe circulaire 10
12. Birapport de quatre points sur une conique et théorème de Pascal 12
13. Propriétés métriques des coniques affines euclidiennes 14
14. Les six birapports de Perrin, droite de Simpson, théorème de Miquel et le pivot 15
15. Idéaux bilatères de $L(E)$ 16
16. A_n est simple pour n supérieur à 5 17
17. Polynômes symétriques 17
18. A propos de $k[X_1,\ldots,X_n]\ldots$ 18
19. Le théorème de Hahn-Banach version géométrique 19
20. Théorème de Jung 20
21. Espace vectoriel de dimension finie 22
22. $\mathbb{F}_q^\star$ est cyclique et quand a-t-on $\mathbb{F}_q \subset \mathbb{F}_{q'}$? 23
23. le rang d'une différentielle 23
24. Ellipsoïde de John 24
25. Un peu de topologie sur les matrices 28

Date: Novembre 2000.

1. Simplicité de $PSL(n,k)$

Cf : Perrin p.102

Théorème 1. *$PSL(n,k)$ est simple sauf dans les deux cas suivants :*

- $n=2$, $k=\mathbb{F}_2$
- $n=2$, $k=\mathbb{F}_3$

Remarques :

(1) Connaître les cas particuliers, par exemple $PSL(2,\mathbb{F}_2)\approx S_3$ (Perrin p.106) donc $PSL(2,\mathbb{F}_2)$ n'est pas simple.
(2) Dans la démonstration on sépare les cas $n\geq 3$ et $n=2$, bien comprendre d'où cela vient, et regarder les pages précédentes dans Perrin où il démontre des résultats relatifs aux groupes linéaires (générateurs, groupes dérivés, centres,...).
(3) Dans cette démonstration comme dans presque toutes les démonstrations de simplicité on connaît les générateurs et leur comportement par conjugaison (par exemple, les générateurs sont conjugués entre eux) puis on suppose par l'absurde qu'il existe un sous-groupe distingué H non réduit au neutre. Ensuite on considère $h\neq Id$ dans H et on regarde les commutateurs $hgh^{-1}g^{-1}$ qui est encore dans H pour tous les g dans le groupe considéré puis on cherche g tel que $hgh^{-1}g^{-1}$ soit un générateur, puis on conclut. Il est évident que lors d'une présentation orale il faut insister sur le caractère général de cette méthode.
(4) Bien comprendre l'interprétation géométrique des transvections et des dilatations.
(5) Bref une bonne lecture du Perrin s'impose!

2. Simplicité de $O^+(3,\mathbb{R})$

Cf : Perrin p.148, Audin p.123 et p.283

Théorème 2. *Le groupe $O^+(3,\mathbb{R})$ est simple.*

Remarques :

(1) Regarder la remarque 3 du paragraphe 1
(2) Dans Audin p.121 exercice 10 (corrigé p.283) il y a des précisions concernant la démonstration du résultat suivant (je reprends les notations de Perrin) : on a y_1 et y_2 dans S^2 tels que $\|y_1-y_2\|=m$ et on veut montrer qu'il existe $u'\in N$ tel que $u'(y_1)=y_2$.
(3) Dans la démonstration on a utilisé que $\mathbb{R}$ est archimédien, voir un contre-exemple dans Perrin p.158 exercice 2.
(4) Connaître quelques propriétés topologiques de $O(E)$ (cf dans Audin p.50 et Arnaudiès T 4 p.70) où E est un $\mathbb{R}$-espace vectoriel de dimension n par exemple :
   - $O(n)$ est compact et $O^+(n)$ est compact.

- $O^+(n)$ est connexe par arcs.
- $O(n)$ a deux composantes connexes.

3. Simplicité de $PO^+(n,\mathbb{R})$ pour $n \geq 5$

Cf : Perrin p.150

Théorème 3. *$PO^+(n,\mathbb{R})$ est simple pour $n = 3$ et $n \geq 5$.*

Remarques :

(1) Regarder la remarque 3 du paragraphe 1.
(2) Si la dimension est impaire, l'existence d'un point fixe pour ρ est clair. En effet il suffit de réduire ρ sous la forme suivante :

$$\begin{pmatrix} Id & 0 & \cdots & \cdots & 0 \\ 0 & -Id & \ddots & & \vdots \\ \vdots & \ddots & R(\theta_1) & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & R(\theta_p) \end{pmatrix}$$

où $R(\theta)$ est une matrice de rotation d'angle θ.
(3) Si N est un sous-groupe distingué de $O(n,\mathbb{R})$ et qu'il contient strictement le centre alors N contient $O^+(n,\mathbb{R})$ dès que $n \geq 3$.

4. Classes d'équivalence dans $M_{n\times p}(A)$ et deux applications

Cf : Artin p.459 pour l'existence, Goblot p.161 pour l'unicité, Jacobson p.182 pour l'application, L.Schwartz p.45 pour les groupes abéliens, Francinou p.3

Théorème 4 (Artin p.459 et Goblot p.161)**.** *Soient A un anneau euclidien et $M \in M_{n,p}(A)$ où le rang de M est r, alors il existe $d_1, \ldots, d_r$ dans A uniques à un inversible près tels que d_i divise d_{i+1} et M soit équivalente à le matrice suivante :*

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & d_r & 0 \\ 0 & \cdots & 0 & ? \end{pmatrix}$$

Le "?" signifie qu'on ne sait pas à priori comment se finit la matrice.

Remarques :

(1) Ce théorème est très important car il a des applications dans différents domaines et donc il crée un "pont suspendu" entre ces domaines.
(2) Ce théorème est encore vrai si l'on suppose A principal (cf Goblot p.161).

(3) La démonstration donne un algorithme constructif cependant il est un peu bizarre : il faut bien expliquer pourquoi il se termine en un nombre fini d'étapes.

Application : (Jacobson p.182) Soient A un anneau euclidien et G un A-module de type fini alors G est isomorphe à $A/(d_1) \oplus \cdots \oplus A/(d_r) \oplus A^q$ avec d_i qui divise d_{i+1} et d_i unique à un inversible près.

Remarques :

(1) Le résultat est aussi vrai pour A principal.
(2) Attention l'unicité des d_i ne résulte pas du théorème précédent, comprendre pourquoi!
(3) Dans la démonstration de l'application on utilise des résultats sur les modules libres de type fini. Par exemple : un sous-module d'un module libre est libre et un sous-module d'un module de type fini est de type fini (Attention il ne faut calquer les propriétés des espaces vectoriels sur les modules).
(4) Selon la forme de la matrice du théorème 4, savoir si le A-module considéré a une partie libre.
(5) Savoir écrire un groupe abélien fini sous cette forme, par exemple $\mathbb{Z}/4 \times \mathbb{Z}/27$, $\mathbb{Z}/4 \times \mathbb{Z}/18\ldots$ et savoir passer de l'écriture $\mathbb{Z}/p_1^{r_1} \times \cdots \times \mathbb{Z}/p_k^{r_k}$ (avec les p_i premiers) à celle proposée ici.

Application : (Schwartz p.45 et Francinou p.3) Soit G un groupe abélien fini, alors il existe $m_1, \ldots, m_n$ dans $\mathbb{Z}$ uniques tels que m_{i+1} divise m_i et G isomorphe $\mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_n$.

Remarques :

(1) Dans Schwartz, il ne justifie pas pourquoi si d divise l'ordre de G alors il existe un unique sous-groupe de G d'ordre d. C'est fait dans Francinou p.3.
(2) Vers la fin de la démonstration, Schwartz ne dit pas clairement qu'il y a une équivalence entre p divise m_n et p divise m'_n.

5. Réduction de Frobenius et réduction de Jordan par les $\mathbb{K}[X]$-module

Cf : Artin p.476, Jacobson p.189

Soit K un corps, on prend $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On note $L(E)$ l'ensemble des endomorphismes de E.

Théorème 5 (Réduction de Frobenius, voir Artin p.476 et Jacobson p.189)**.** *Soient E un $\mathbb{K}$-espace vectoriel de dimension n et $f \in L(E)$ alors (E, f) est isomorphe comme $\mathbb{K}[X]$-module à $\mathbb{K}[X]/(P_1) \oplus \cdots \oplus \mathbb{K}[X]/(P_r)$ où les P_i sont des polynômes unitaires dans $\mathbb{K}[X]$ tels que P_i divise P_{i+1}. Les P_i sont uiniques.*

De plus la matrice de f est semblable à

$$\begin{pmatrix} M_1 & & \boldsymbol{0} \\ & \ddots & \\ \boldsymbol{0} & & M_r \end{pmatrix}$$

où M_i est la matrice compagnon de P_i.

Remarques :

(1) Quand j'écris (E, f) cela signifie que considère E comme muni de la structure de $\mathbb{K}[X]$-module définie par f. Ainsi dès qu'on démontre un résultat de structure sur les modules (cf le théorème 4) on peut le transposer en algèbre linéaire par l'intermédiaire des $\mathbb{K}[X]$-modules (cf Artin p.476)[1]. La clé de la démonstration est le théorème 4.

(2) Cette réduction peut être obtenue directement (cf Gourdon algèbre p.281) mais cela cache la jolie forêt des $\mathbb{K}[X]$-modules.

(3) Ce qu'il faut bien comprendre c'est que (E, f) et (F, g) sont isomorphes comme $\mathbb{K}[X]$-modules si et seulement si f et g sont conjugués (par un élément de $GL(E)$).

(4) Les P_i sont appelés les invariants de similitudes car deux endomorphismes sont semblables si et seulement si ils ont les mêmes invariants de similitudes (encore heureux!).

(5) Le polynôme caractéristique c'est $(-1)^n P_1 \cdots P_r$ et le polynôme minimal c'est P_r, pourquoi ?

Application : Réduction de Jordan, cf Artin. Soient $\mathbb{K} = \mathbb{C}$ et $A \in M_n(\mathbb{C})$ alors A est équivalente à la matrice :

$$\begin{pmatrix} J_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & J_p \end{pmatrix} \text{ où } J_i(\lambda_i) = \begin{pmatrix} \lambda_i & 0 & \cdots & 0 \\ 1 & \ddots & \ddots & \vdots \\ & \ddots & \ddots & 0 \\ \mathbf{0} & & 1 & \lambda_i \end{pmatrix}.$$

Remarque : Comment faire pour passer d'une décomposition de Jordan à la réduction de Frobenius ? Regarder dans Jacobson p.185 (il le fait sur les groupes abéliens finis mais c'est la même méthode). Prenons un exemple : soit la matrice

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

[1] et en théorie des groupes, les groupes abéliens étant les $\mathbb{Z}$-modules.

Les polynômes qui interviennent dans la décomposition de Jordan sont $X-1$, $(X-2)^2$, $(X-3), (X-3)$ et $(X-3)^2$, ainsi $P_3 = (X-1)(X-2)^2(X-3)^2$, $P_2 = (X-3)$ et $P_1 = (X-3)$. Voir la remarque 5 du §4.

6. Théorèmes de Sylow

Cf : Artin p.205, Calais p.208, Perrin

Théorème 6 (Existence, Artin)**.** *Soit G un groupe de cardinal n où $n = p^e m$ avec p premier ne divisant pas m alors G contient un sous-groupe de cardinal p^e. Un tel sous-groupe est appelé un p-sous-groupe de Sylow.*

Théorème 7.
- *Tout p-sous groupe de G est contenu dans un p-Sylow de G.*
- *Les p-Sylow sont tous conjugués.*

Théorème 8. *Le nombre de p-Sylow de G noté n_p est congru à 1 modulo p et n_p divise $\#G$.*

Remarques :

(1) Développement très classique, donc si on peut l'éviter c'est bien, sinon il est impératif de très bien le présenter.
(2) Dans Perrin, il déduit l'existence des p-Sylow du calcul du cardinal de $GL(n, \mathbb{F}_p)$: c'est très astucieux.
(3) Il est quand même bon de revoir les démonstrations des théorèmes de Sylow car elles font intervenir les actions de groupes (cf Francinou pour faire des exercices sur les actions de groupes).

7. Décomposition polaire de $GL(n, \mathbb{R})$

Cf : Mneimné Testard Introduction à la théorie des groupes de Lie classiques p.18, Gourdon algèbre p.246

On note S^{++} l'ensemble des matrices symétriques définies positives.

Théorème 9. *Soit $M \in GL(n, \mathbb{R})$ alors il existe un unique couple (O, S) dans $O(n) \times S^{++}$ tel que $M = OS$.*

Remarques :

(1) Dans cette démonstration, on est attendu sur l'unicité donc il faut l'expliquer clairement.
(2) Si M n'est pas inversible, alors on a encore l'existence de $O \in O(n)$ et S symétrique positive (mais pas définie), mais pas avec cette démonstration et l'unicité est perdue à jamais.

Lemme 1. *$O(n)$ est compact.*

Théorème 10. *L'application suivante est un homéomorphisme.*

$$\begin{array}{ccc} O(n) \times S^{++} & \longrightarrow & GL(n, \mathbb{R}) \\ (O, S) & \longmapsto & OS \end{array}$$

Remarque : De ce théorème on en déduit l'existence de la décomposition polaire pour M dans $M(n,\mathbb{R})$. En effet comme $GL(n,\mathbb{R})$ est dense dans $M(n,\mathbb{R})$ alors on prend une suite $(M_p)_{p\in\mathbb{N}}$ qui converge vers M. Pour tout p dans $\mathbb{N}$ on a l'existence d'un couple (O_p, S_p) dans $O(n)\times S^{++}$ tel que $O_pS_p = M$. Puis la compacité de $O(n)$ permet d'extraire une sous-suite $(O_{p_k})_{k\in\mathbb{N}}$ qui converge vers $O\in O(n)$. On pose alors $S = O^{-1}M$ et on a $(S_{p_k})_{k\in\mathbb{N}}$ qui converge vers S qui est dans S^+.

8. Théorème des zéros de Hilbert

Cf : Artin p.371

Théorème 11. *Les idéaux maximaux de $\mathbb{C}[X_1,\dots,X_n]$ sont en correspondance bijective avec les points de $\mathbb{C}^n$. A un point $a = (a_1,\dots,a_n)\in\mathbb{C}^n$ correspond le noyau de s_a où s_a est l'application suivante :*

$$\begin{array}{rccc} s_a\ : & \mathbb{C}[X_1,\dots,X_n] & \longrightarrow & \mathbb{C} \\ & f & \longmapsto & f(a) \end{array}$$

Le noyau noté M_a de s_a est l'idéal engendré par $x_1-a_1,\dots,x_n-a_n$.

Remarque : Ce théorème est important car il relie les variétés algébriques (c'est-à-dire les zéros communs d'un nombre fini de polynômes de $\mathbb{C}[X_1,\dots,X_n]$) à l'algèbre. La démonstration utilise beaucoup de résultats basiques, cependant j'ai eu du mal à le mettre dans les leçons. Mais comme on est aussi jugé sur notre culture mathématique c'est tout de même un plus.

9. Sous groupes finis de $O(2,\mathbb{R})$ et de $O(3,\mathbb{R})$

Cf : Arnaudiès 5 polyèdres réguliers p.56, Artin p.162

Théorème 12. *Soit G un sous groupe fini de $O(2,\mathbb{R})$ alors soit G est cyclique soit G est un groupe diédral.*

Théorème 13. *Soit G un sous groupe fini de $O^+(3,\mathbb{R})$ alors on a soit*

(1) $G\approx\mathbb{Z}/n\mathbb{Z}$
(2) $G\approx D_{2n}$
(3) $G\approx A_4$
(4) $G\approx S_4$
(5) $G\approx A_5$

Remarque : Très belle démonstration et très joli résultat, noter que dans la démonstration on montre que A_5 est simple.

Corollaire 1. *Soit G un sous groupe fini de $O(3,\mathbb{R})$ et $G\not\subseteq O^+(3,\mathbb{R})$ alors on note $G^+ = G\cap O^+(3,\mathbb{R})$ et $G\approx G^+\rtimes\{\pm Id\}$ et si $-Id\in G$ alors le produit est direct.*

Remarque : Les différentes approches (section, action de groupe et définition standard cf Perrin et Francinou) du produit semi-direct doivent être bien comprises.

10. Loi de réciprocité quadratique par le lemme chinois

Cf : Serre p.15, Gozard p.93, Gourdon algèbre p.46, RMS mars 1990 p.339. Dans Gozard il y a la définition du symbole de Legendre et quelques propriétés.

Théorème 14. *Pour p et q deux nombres premiers distincts différents de 2, on a*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Preuve : Elle n'est faite nulle part à ma connaissance. D'après le lemme chinois on a :

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \approx \mathbb{Z}/pq\mathbb{Z}, \text{ donc } \mathbb{Z}/p\mathbb{Z}^\star \times \mathbb{Z}/q\mathbb{Z}^\star \approx \mathbb{Z}/pq\mathbb{Z}^\star.$$

Notons $G \approx \mathbb{Z}/pq\mathbb{Z}^\star$ et $U = \{\pm 1\}$. L'idée est de faire le produit de tous les éléments de G/U (pourquoi pas !).

On regarde d'abord le produit dans $\mathbb{Z}/p\mathbb{Z}^\star \times \mathbb{Z}/q\mathbb{Z}^\star/\{\pm(1,1)\}$. Les éléments de G/U ont un représentant de la forme (k,l) où $1 \leq k \leq p-1$ et $1 \leq l \leq \frac{q-1}{2}$ (comprendre pourquoi). On a bien $(p-1)(q-1)/2$ éléments. Le produit donne

$$\left((p-1)!^{\frac{q-1}{2}}, \left[\left(\frac{q-1}{2}\right)!\right]^{p-1}\right).$$

Or

$$(q-1)! = 1 \ldots \frac{q-1}{2}\frac{q+1}{2}\ldots(q-1)$$

et dans $\mathbb{Z}/q\mathbb{Z}$ on a

$$\frac{q+1}{2} = \frac{q+1}{2} - q = -\frac{q-1}{2} \text{ donc } (q-1)! = \left[\left(\frac{q-1}{2}\right)!\right]^2.$$

Ainsi

$$\left(\frac{q-1}{2}\right)!^{p-1} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(q-1)!^{\frac{p-1}{2}}$$

et donc le produit vaut :

$$\left((p-1)!^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(q-1)!^{\frac{p-1}{2}}\right)$$

On regarde ensuite le produit dans $(\mathbb{Z}/pq\mathbb{Z})^\star/\{\pm 1\}$, qui vaut

$$P = \frac{\left(\frac{pq-1}{2}\right)!}{\left(p \cdot 2p \ldots \frac{q-1}{2}p\right) \cdot \left(q \cdot 2q \ldots \frac{p-1}{2}q\right)}.$$

Le numérateur est le produit des éléments de $(\mathbb{Z}/pq\mathbb{Z})/\{\pm 1\}$ et au dénominateur on a les éléments non inversibles de $\mathbb{Z}/pq\mathbb{Z}$ inférieurs à $(pq-1)/2$;

Ainsi en simplifiant par p, $2p, \dots, p(q-1)/2$ on a :

$$P = \frac{\left(\prod_{i=1}^{p-1} i\right) \cdot \left(\prod_{i=1}^{p-1} p+i\right) \dots \left(\prod_{i=1}^{p-1} \frac{q-3}{2}p+i\right) \cdot \left(\prod_{i=1}^{\frac{p-1}{2}} \frac{q-1}{2}p+i\right)}{q \cdot 2q \dots \frac{p-1}{2}q}.$$

Noter que la fraction a bien un sens car les termes du dénominateur apparaissent au numérateur. Puis on regarde cette égalité modulo p : on a alors

$$\begin{aligned}
P &\equiv \frac{(p-1)!^{\frac{q-1}{2}} \cdot \prod_{i=1}^{\frac{p-1}{2}} \left(\frac{q-1}{2}p+i\right)}{q^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!} && \mod p \quad \text{car } p+i \equiv i \mod p \\
&\equiv \frac{(p-1)!^{\frac{q-1}{2}} \cdot \left(\frac{p-1}{2}\right)!}{q^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!} && \mod p \\
&\equiv \frac{(p-1)!^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} && \mod p \\
&\equiv (p-1)!^{\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right) && \mod p \quad \text{car } q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right)
\end{aligned}$$

De même on réduit P modulo q et on a : $P \equiv (q-1)!^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right) \mod q$.

Ainsi dans G/U on a l'égalité suivante :

$$\left((p-1)!^{\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right)\right) = \left((p-1)!^{\frac{q-1}{2}}, (q-1)!^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\right)$$

car $\left(\frac{p}{q}\right) = \pm 1$ et $(x,y) = (-x,-y)$ dans G/U. Ainsi quand on relève cette égalité dans $\mathbb{Z}/q\mathbb{Z}$ on a :

$$(-1)^{\frac{q-1}{2}\frac{p-1}{2}}(q-1)!^{\frac{p-1}{2}} = (q-1)!^{\frac{p-1}{2}} \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \mod q$$

c'est-à-dire $(-1)^{\frac{q-1}{2}\frac{p-1}{2}} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \mod q$. Et comme $q \neq 2$ on a

$$(-1)^{\frac{q-1}{2}\frac{p-1}{2}} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

Remarques :

(1) Faire attention quand on passe d'une égalité dans G/U à une égalité dans $\mathbb{Z}$.

(2) La démonstration marche mais je ne sais pas trop pourquoi, c'est gênant, cependant je n'ai toujours pas compris pourquoi la loi de réciprocité quadratique est "intuitivement" vraie. Les autres démonstrations de cette loi sont toutes aussi[2] obscures mais elles font intervenir des outils plus puissants que la multiplication !
(3) Le problème des carrés dans les anneaux non intègres est plus complexe (cf le symbole de Jacobi). Par exemple dans $\mathbb{Z}/8\mathbb{Z}$ l'équation $x^2 = 1$ admet 4 solutions donc la même démonstration ne colle plus !

Théorème 15 (Serre p.15)**.** *Pour p premier strictement supérieur à 2, on a*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Application : [Un test de primalité, Gourdon algèbre p.46]

(1) Soient h et m deux entiers tels que $m \geq 2$ et $1 \leq h \leq 2^m - 1$, on pose $n = 2^m h + 1$. Soit $p > 2$ premier tel que $\left(\frac{n}{p}\right) = -1$, on a alors l'équivalence suivante : n est premier si et seulement si $p^{\frac{n-1}{2}} = -1 \mod n$.
(2) On a aussi l'équivalence suivante : $F_k = 2^{2^k} + 1$ est premier si et seulement si $3^{\frac{F_k-1}{2}} \equiv -1$ modulo F_k.

Application : [RMS 89-90 mars 1990 p.339] Soient p un nombre premier strictement supérieur à 2 et $a \neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$, on a alors l'équivalence suivante : a est un carré modulo p si et seulement si σ_a est une permutation paire. Où σ_a est définit par :

$$\begin{array}{rccc} \sigma_a & : & \mathbb{Z}/p\mathbb{Z}^\star & \longrightarrow & \mathbb{Z}/p\mathbb{Z}^\star \\ & & b & \longrightarrow & ab \end{array}$$

11. Le groupe circulaire

Cf : Audin p.155, Samuel p.103.

Définition 1. *Le groupe circulaire est le groupe de transformations de $\mathbb{P}_1(\mathbb{C})$ engendré par les transformations de $P_1(\mathbb{C})$ suivantes :*

- $z \longrightarrow \dfrac{az+b}{cz+d}$ *avec* $ad - bc \neq 0$,
- $z \longrightarrow \overline{z}$.

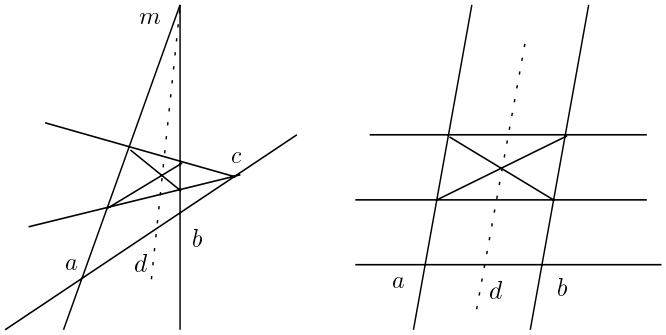
Proposition 1. *Le groupe circulaire est engendré par les inversions et les réflexions.*

Théorème 16 (Audin p.155)**.** *Les éléments du groupe circulaire sont les applications bijectives de $P_1(\mathbb{C})$ dans $P_1(\mathbb{C})$ qui préservent l'ensemble des cercles et droites.*

[2] ou tout aussi

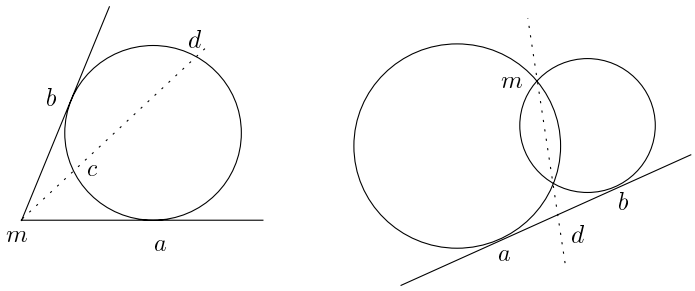
Compléments sur la preuve :

(1) Tout d'abord je vais expliquer la "contemplation" de la page 156 :
   (a) Si a, b et c sont alignés : on contemple la figure de gauche, qu'on transforme en celle de droite.



ATTENTION on utilise que le birapport réel et le même que le birapport complexe : en effet on considère (ab) comme $P_1(\mathbb{R})$ et on a $[a,b,c,d]_{\mathbb{R}} = [a,b,c,d]_{\mathbb{C}}$ car $PGL(2,\mathbb{R}) \subset PGL(2,\mathbb{C})$. Puis l'idée est de regarder le dessin dans $P_2(\mathbb{R})$. On envoie donc **UNE DROITE** à l'infini en l'occurrence la droite (mc). C'est la figure de droite. Et il est clair que d est le milieu de $[ab]$ ainsi $[a,b,\infty,d] = [a,b,d,\infty]^{-1} = (-1)^{-1} = -1$.

   (b) Si a, b et c sont cocycliques : on contemple à nouveau la figure de gauche, qu'on va transformer en celle de droite.



On considère cette fois que le dessin est dans $P_1(\mathbb{C})$ et on envoie donc **UN POINT** à l'infini en l'occurrence le point c. Les droites (ma) et(mb) deviennent des cercles tangents à la droite ab, image du cercle C circonscrit à abc.
Le point d est sur l'axe radical des deux cercles transformés de ma et mb, on a donc $\|\overrightarrow{da}\|^2 = \|\overrightarrow{db}\|^2$, en d'autre termes d est le

milieu de $[ab]$ donc $[a,b,c,d] = -1$. On conclut en utilisant les hypothèses suivante :

- φ envoie un cercle sur un cercle et une droite sur une droite.
- φ est bijective.

Donc les deux figures sont préservées par φ, ainsi φ préserve les divisions harmoniques.

(2) Pour le lemme p.156 il faut rajouter les hypothèses $\varphi(0) = 0$ et $\varphi(1) = 1$

(3) Puis pour conclure (regarder dans Samuel p.78), on sait que :

- $\varphi(\infty) = \infty$.
- φ conserve les cercles.
- φ conserve les droites.

Ainsi quitte à composer par une similitude directe on peut supposer que $\varphi(0) = 0$ et $\varphi(1) = 1$. D'où φ préserve l'axe réel. Par conséquent φ est un automorphisme de $\mathbb{C}$ qui préserve l'axe réel. Un petit raisonnement[3] montre que φ est croissant (cf Samuel) ainsi φ est l'identité ou le conjugaison.

12. Birapport de quatre points sur une conique et théorème de Pascal

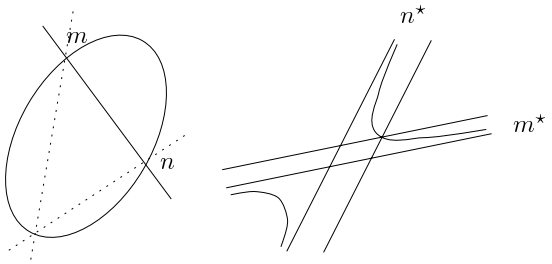
Cf : Audin p.194, Berger T 2 p.270.

12.1. **Théorème de Pascal.** Soit C une conique et $m \in C$, le point m définit une application

$$\pi_m \ : C \longrightarrow m^\star$$

qui, au point n de C, associe la droite (mn).

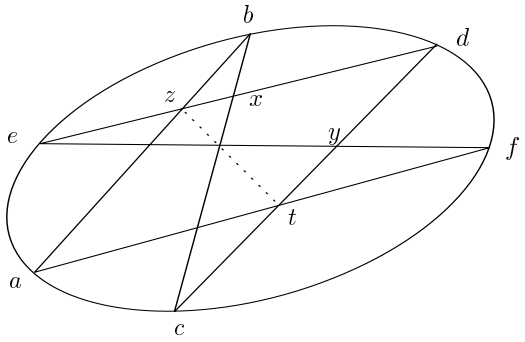
Proposition 2. *Soit C une conique non dégénérée d'image non vide alors π_m est une bijection et $\pi_n \circ \pi_m^{-1} \ : m^\star \longrightarrow n^\star$ est une homographie.*



[3]... classique, on détermine les automorphismes de corps de $\mathbb{C}$ qui préservent $\mathbb{R}$.

Preuve : La preuve que je donne a été proposée en oral blanc l'année passée (le choix de coordonnées dans Audin est un peu trop compliqué) et en cherchant bien il se pourrait qu'elle ressemble à celle de Berger T 2 p.270 (ça reste à voir !). On se place dans $P_2(\mathbb{R})$ et on envoie la droite (mn) à l'infini. La figure devient plus simple : la conique devient une hyperbole d'équation $xy = a$ dans le repère formé par ses asymptotes. $m^\star$ est l'ensemble des droites parallèles à une asymptote et $n^\star$ est l'ensemble des droites parallèles à l'autre asymptote. Ainsi l'application $\pi_n \circ \pi_m^{-1}$ envoie $x \in m^\star$ sur $a/x \in n^\star$ qui est une homographie ($m^\star$ c'est $\mathbb{R} \cup \{\infty\}$).

Corollaire 2. *Soit C une conique non dégénérée d'image non vide et soient m_1, m_2, m_3 et m_4 dans C, alors $[mm_1, mm_2, mm_3, mm_4]$ ne dépend pas de m dans C.*



Théorème 17. *Soit C une conique d'image non vide et non dégénérée, soient $a, b, c, d, e, f \in C$ alors $(ab) \cap (dc)$, $(bc) \cap (ef)$ et $(cd) \cap (fa)$ sont alignés.*

Remarques :

(1) L'énoncé dual de Pascal c'est le théorème de Brianchon.
(2) Si la conique C est dégénérée (deux droites distinctes) alors le théorème de Pascal c'est le théorème de Pappus (cf Audin exo 48 p.216)[4].
(3) A partir de cinq points distincts sur une conique C, construire un point arbitraire de C et la tangente en ce point (cf Audin exo 50 p.216). Si les cinq points sont "assez généraux", ils déterminent une unique conique et le théorème de Pascal permet de construire les points de cette conique (et la tangente en ces points).
(4) Quand on veut présenter un développement de géométrie il faut faire des figures, et donc il faut s'entraîner à les dessiner et à prendre les bonnes notations.

[4]Ne pas placer les six points n'importe comment sur les trois droites !

12.2. **Dual d'une conique.** Cf : Samuel p.136. Dans la remarque précédente je parle d'un énoncé dual au théorème de Pascal, or le dual d'une conique non dégénérée est encore une conique non dégénérée (c'est exactement l'énoncé du théorème suivant). Soit Q une forme quadratique non dégénérée sur E qui définit une conique C et $\tilde{\varphi}$ l'isomorphisme associé de E dans $E^\star$.

Théorème 18. *On pose $Q^\circ(u) = Q(\tilde{\varphi}^{-1}(u))$ pour tout u dans $E^\star$. L'hyperplan H d'équation $u(x) = 0$ est tangent à C si et seulement si $Q^\circ(u) = 0$.*

Preuve : On note C° la conique définie par Q°. On a alors les équivalences suivantes :

$$\begin{aligned} u \in C^\circ &\iff Q(\tilde{\varphi}^{-1}) = 0 \\ &\iff \tilde{\varphi}^{-1} \in C \\ &\iff u \in \tilde{\varphi}(C) \text{ car } \tilde{\varphi} \text{ est un isomorphisme.} \\ &\iff \exists x_0 \in C \text{ tel que } \tilde{\varphi}(x_0) = u. \end{aligned}$$

Ainsi on a les équivalences suivantes :

$$\begin{aligned} x \in H &\iff \tilde{\varphi}(x_0)(x) = 0 \\ &\iff x \in x_0^\perp \\ &\iff \text{H est l'hyperplan tangent à } C \text{ en } x_0. \end{aligned}$$

De plus si on note φ° la forme bilinéaire associée à C° alors on a

$$\tilde{\varphi}^{-1} = \varphi\left(\tilde{\varphi}^{-1}(x), \tilde{\varphi}^{-1}(y)\right)$$

pour tout $x, y \in E^\star$. Ainsi $\tilde{\varphi}$ est non dégénérée c'est-à-dire C° est une conique propre.

Remarques :

(1) Si on veut définir une forme quadratique Q° sur $E^\star$ à partir d'une forme quadratique Q non dégénérée sur E, ben on n'a pas le choix il faut poser $Q^\circ(u) = Q(\tilde{\varphi}^{-1}(u))$ pour tout u dans $E^\star$.
(2) Le théorème dit que l'ensemble des hyperplans tangents à une quadrique non dégénérée est une quadrique non dégénérée dans le dual.

Corollaire 3. *Si M est la matrice de φ dans la base canonique de E alors la matrice de φ° est M^{-1} dans la base "canonique duale" de $E^\star$.*

Voir Samuel.

13. Propriétés métriques des coniques affines euclidiennes

Cf : Audin p.199

Lemme 2 (Audin p.187)**.** *Si D est une droite projective (en dimension 1) et C une quadrique propre d'image non vide de D, elle est formée de 2 points a et b alors on a l'équivalence suivante : $[a, b, m, n] = -1$ si et seulement si $M \perp_Q n$ où Q est la forme quadratique qui définit C.*

On note I et J les points cycliques.

Théorème 19 (Audin p.199)**.** *On va distinguer deux cas selon la nature de C.*

(1) *Soit C une parabole, la droite (IJ) est tangente à C. La deuxième tangente à C issue de I et la deuxième tangente à C issue de J se coupent au foyer F de la parabole.*
(2) *Soit C une conique à centre qui n'est pas un cercle. Soient D_1 et D_2 les tangentes à C passant par I, D_1' et D_2' les droites complexes* ***conjuguées respectives*** *de D_1 et D_2. Les droites D_1' et D_2' sont les tangentes à C issue de J et les foyers de C sont les points $F_1 = D_1 \bigcap D_1'$ et $F_2 = D_2 \bigcap D_2'$. De plus les polaires de F_1 et F_2 par rapport à C sont les directrices correspondantes.*

Remarques :

(1) Cette démonstration est courte mais dense : on utilise beaucoup de résultats sur les coniques, les birapports et les homographies.
(2) Pourquoi peut-on mener deux tangentes à une conique à partir d'un point extérieur à cette conique?
— Si on considère la conique duale (cf le paragraphe 12.2) et qu'on remarque qu'une droite coupe une conique en deux points, alors on a le résultat directement.

14. Les six birapports de Perrin, droite de Simpson, théorème de Miquel et le pivot

Cf : Audin p.163

Proposition 3. *Soient huit points $A, B, C, D, A', B', C' et D'$ dans $P_1(\mathbb{C})$, on a alors*

$$[A, B, C', D'][B, C, A', D'][C, A, B', D'][A', B', C, D][B', C', A, D][C', A', B, D] = 1$$

Cette proposition a des conséquences surprenantes :

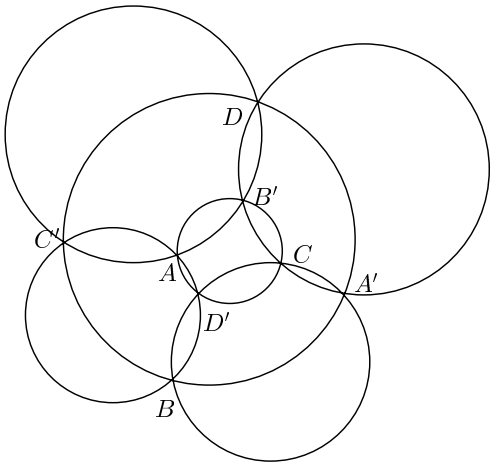
Théorème 20 (Théorème de Miquel, Audin p.97)**.** *Soient quatre cercles C_1, C_2, C_3 et C_4 tels que :*

$C_1 \cap C_4 = \{A, C'\}$, $C_1 \cap C_2 = \{D', B\}$, $C_2 \cap C_3 = \{C, A'\}$ *et* $C_3 \cap C_4 = \{B', D\}$.

On a l'équivalence suivante : A, B', C et D' sont cocycliques si et seulement si A', B, C' et D le sont.

Proposition 4 (La droite de Simson, Audin p.97)**.** *Soient ABC un triangle et M un point du plan, soient P, Q et R les projetés orthogonaux de M sur les droites (BC), (CA) et (AB), on a l'équivalence suivante : P, Q et R sont alignés si et seulement si M est sur le cercle circonscrit au triangle.*

Proposition 5 (Le pivot, Audin p.98)**.** *Soient ABC un triangle et A', B' et C' trois points distincts situés respectivement sur les segments $[BC]$, $[AC]$ et $[AB]$ différent de A, B et C, alors les cercles circonscrits à $AB'C', BC'A'$ et $CA'B'$ ont un point commun.*



Remarque : C'est un bon développement original, pas dur et qui démontre astucieusement des résultats de géométrie classique. Par contre, il faut faire attention à la numérotation des points.

15. Idéaux bilatères de $L(E)$

Cf : Goblot p.113. Soit E un k-espace vectoriel où $k = \mathbb{R}$ ou $\mathbb{C}$. On va regarder comment se comportent les idéaux bilatères de $L(E)$ selon la dimension de E.

Proposition 6. (i) *Si la dimension de E est finie alors les idéaux bilatères de $L(E)$ sont triviaux.*

(ii) *Si la dimension de E est infinie alors $I = \{f \in L(E)$ tel que $rg(f) < +\infty\}$ est un idéal bilatère non trivial de $L(E)$ et c'est le plus petit non trivial.*

(iii) *Si la dimension de E est dénombrable : le seul idéal bilatère non trivial est I.*

(iv) *Si la dimension de E est non dénombrable alors il y a d'autres idéaux bilatères.*

Remarques :

(1) Dans la démonstration on utilise un autre lemme de manière tacite : soit $f \in L(E)$ et S un supplémentaire de $\ker f$ dans E alors $\operatorname{Im} f \approx S$. En effet $f_{|S} : S \longrightarrow \operatorname{Im} f$ est clairement injective et pour $y \in \operatorname{Im} f$ il existe $x \in E$ tel que $y = f(x)$ et $x = t + s$ avec $s \in \ker f$ et $t \in S$ donc $f(x) = f(t) = y$ (ceci démontre aussi le théorème du rang).

(2) Dans un développement il faut éviter de dire "par un lemme trivial, on a..." ou "un calcul facile montre..." car si c'est facile alors faites-le, ben Dieu !
(3) Avoir une petite idée sur les idéaux monolatères de $L(E)$ en dimension finie.

16. A_n est simple pour n supérieur à 5

Cf : Perrin. On note A_n le groupe alterné à n éléments.

Théorème 21. *A_n est simple pour n supérieur ou égal à 5.*

Remarques :

(1) Attention les éléments d'ordre 5 dans A_5 ne sont pas tous conjugués entre eux car 24 ne divise pas 60, par contre si a et b sont d'ordre 5 alors a est conjugué à b ou à b^2.
(2) Dans la démonstration on a utilisé deux résultats importants :
   (a) Les 3-cycles sont tous conjugués dans A_n.
   (b) Les 3-cycles engendrent A_5.

Corollaire 4. *On a $D(A_n) = A_n$ pour n supérieur à 5.*

Remarque : En fait ces résultats sont très importants car ils permettent de démontrer modulo la théorie de Galois l'impossibilité de résoudre une équation générale de degré 5 par radicaux. Revoir ce que cela signifie "être résoluble par radicaux" et "équation générale de degré n". Savoir aussi le théorème fondamental suivant :

Théorème 22. *Soit $f \in K[X]$. L'équation $f(X) = 0$ est résoluble par radicaux sur K si et seulement si le groupe de Galois de f est résoluble.*

Remarque : Il est bien évident qu'il faut juste connaître les définitions et les liens entre ces notions et non pas les démonstrations entières : la théorie de Galois n'est pas au programme de l'agrégation. Pour les étudiants qui n'ont jamais fait de théorie de Galois, ne perdez votre temps là-dessus même si c'est très joli (sauf si c'est votre dernière lacune!).

17. Polynômes symétriques

Cf : Jacobson p.133, Tauvel p.122.

Théorème 23. (i) *Soit A un anneau commutatif, tous les polynômes symétriques sur $A[X_1, \ldots, X_n]$ peuvent s'exprimer à partir des polynômes symétriques élémentaires.*
(ii) *Les polynômes symétriques élémentaires sont algébriquement indépendants sur A.*
(iii) *Tout x_i est algébrique sur $A[p_1, \ldots, p_n]$ où les p_i sont les polynômes symétriques élémentaires.*

Remarque :

(1) Si A est un corps K, on peut dire que l'extension
$$K(X_1, \ldots, X_n)/K(p_1, \ldots, p_n)$$
est algébrique de degré $n!$.
(2) (ii) donne l'unicité de la décomposition de (i).
(3) Après un tel théorème, la question naturelle du jury est : soit le polynôme $P = X^3 + Y^3 + Z^3$, exprimer P en fonction des polynômes symétriques élémentaires (cf Gourdon algèbre p.79 et Tauvel p.122).

Exercice : (cf Tauvel p.122)
On note $f_1, \ldots, f_n$ les n fonctions de $M_n(\mathbb{C})$ dans $\mathbb{C}$ telles que le polynôme caractéristique χ_A de $A \in M_n(\mathbb{C})$ s'écrive :
$$X^n - f_1(A)X^{n-1} + \ldots + (-1)^{n-1} f_{n-1}(A)X + (-1)^n f_n(A)$$
Soit g une fonction polynôme de $M_n(\mathbb{C})$ dans $\mathbb{C}$ telle que $g(AB) = g(BA)$. Montrer que g est un polynôme en $f_1, \ldots, f_n$.

18. A propos de $k[X_1, \ldots, X_n]$...

Je ne connais pas de référence pour le théorème suivant.

Théorème 24. *Si k est un corps, $k[X_1, \ldots, X_n]$ est isomorphe comme k-algèbre à $k[X_1, \ldots, X_m]$ si et seulement si $n = m$.*

Remarque : Ce résultat paraît simple et naturel, mais comment le démontrer sans utiliser le degré de transcendance car il faut suivre le fameux proverbe méta-mathématique suivant : "un résultat trivial doit avoir une démonstration triviale[5]".

Lemme 3. *Si on note H_d l'ensemble des polynômes homogènes de degré d de $k[X_1, \ldots, X_n]$ alors la dimension de H_d est C^d_{n+d-1}.*

Preuve du théorème : Si $m = n$ alors on a clairement un isomorphisme. Réciproquement, on suppose que $m > n$ et que φ réalise un isomorphisme de k-algèbres entre $k[X_1, \ldots, X_m]$ et $k[X_1, \ldots, X_n]$. Ainsi si on restreint φ à $k[X_1, \ldots, X_{n+1}]$ on a un morphisme injectif de k-algèbre de $k[X_1, \ldots, X_{n+1}]$ vers $k[X_1, \ldots, X_n]$. On pose alors : E_d^{n+1} l'ensemble des polynômes de $k[X_1, \ldots, X_{n+1}]$ de degré inférieur ou égal à d (le degré total). On va calculer la dimension de E_d^{n+1}. Pour cela, on considère l'isomorphisme f suivant :
$$\begin{array}{rccc} f & : & E_d^{n+1} & \longrightarrow & H_d^{n+2} \subset k[X_1, \ldots, X_{n+1}, Y] \\ & & X_1^{i_1} \ldots X_{n+1}^{i_{n+1}} & \longmapsto & X_1^{i_1} \ldots X_{n+1}^{i_{n+1}} Y^{d-i_1-\ldots-i_{n+1}} \end{array}$$
En fait f homogénéise les polynômes. Comme f est un isomorphisme on a, d'après le lemme 3, $\dim E_d^{n+1} = C^d_{n+d+1}$. Puis on restreint φ à E_d^{n+1} et on pose $M = \max_{i \in \{1,\ldots,n+1\}} deg(\varphi(X_i))$. On remarque que $\varphi(E_d^{n+1})$, qui est de

[5] ne serait-ce pas la définition d'un résultat trivial?

dimension C^n_{n+d+1},est inclus dans $E^n_{M\cdot d}$ de plus la dimension de $E^n_{M\cdot d}$ est C^{Md}_{Md+n}. Or

$$C^n_{n+d+1} = \frac{(n+d+1)!}{d!(n+1)!} = \frac{(n+d+1)\dots(d+1)}{(n+1)!} \sim_{d\to+\infty} C\cdot d^{n+1}$$

et

$$C^{Md}_{Md+n} = \frac{(Md+n)\dots(Md+1)}{n!} \sim_{d\to+\infty} C'\cdot d^n$$

Ainsi pour d assez grand φ ne peut pas être injectif.

Preuve du lemme : On constate que l'ensemble des monômes $X_1^{i_1}\dots X_n^{i_n}$ tels que $i_1+\dots+i_n = d$ est une base de H_d. Ainsi la dimension de H_d est le cardinal de l'ensemble suivant :

$$\{(i_1,\dots,i_n)\in\mathbb{N}^n \text{ tel que } i_1+\dots+i_n = d\}.$$

Ce cardinal est connu, c'est C^d_{d+n-1} (cf combinaison avec répétitions).

N.B. : La démonstration du lemme a déjà été posée à l'écrit.

Remarque : Concernant les combinaisons avec répétition on peut soit faire un raisonnement combinatoire en plaçant d boules dans $d+n+1$ cases ou on peut aussi les calculer avec les séries génératrices.

19. Le théorème de Hahn-Banach version géométrique

Cf : Berger T2 p.33

Théorème 25. *Soient X un espace vectoriel normé de dimension finie, A un ouvert convexe non vide de X et L un sous espace vectoriel de X tel que $A\cap L = \emptyset$, alors il existe un hyperplan de X qui contient L et qui ne rencontre pas A.*

Remarques :

(1) Je donne un énoncé en dimension finie car la géométrie pour moi c'est plutôt en dimension finie ainsi on évite le lemme de Zorn dans le début de la démonstration.
(2) Dans la démonstration on utilise la projection p de X dans X/M où on munit X/M de la topologie quotient ainsi p est continue et comme A est ouvert, $p(A)$ est ouvert : pourquoi p est ouverte[6]? Revoir les ouverts saturés.
(3) Attention Berger affirme, mais l'agrégatif, lui, il démontre. Par exemple pourquoi $C = \bigcup_{\lambda>0} \lambda B$ est convexe ?

Corollaire 5. *Dans un espace affine X, soient A et B deux convexes non vide, A est ouvert et $A\cap B = \emptyset$, alors il existe un hyperplan séparant A et B.*

[6]Attention, c'est parce qu'on fait le quotient par l'espace vectoriel M que p est ouverte. Il n'est pas vrai que toutes les applications quotient sont ouvertes.

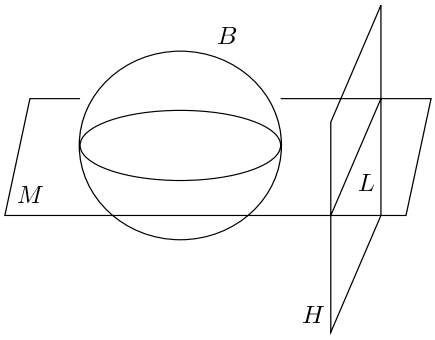
Corollaire 6. *Soient A et B deux convexes non vide, A fermé et B compact tel que $A \cap B = \emptyset$, alors il existe un hyperplan séparant strictement A et B.*

Remarque : Regarder la définition d'un hyperplan d'appui et connaître quelques théorèmes. Ne pas oublier les contre-exemples.

Montrons Hahn-Banach analytique à partir de la version géométrique Je ne connais pas de référence pour cette démonstration. Soient $M \subset X$ où X est un espace vectoriel normé, M un sous-espace de X et f une forme linéaire continue sur M, on considère l'ensemble L des éléments de M tels que $f(x) = 1$.

L'espace L est un sous-espace affine de X et c'est un hyperplan de M. Soit $B = \{x \in X \text{ tel que } \|x\| < \frac{1}{\|f\|}\}$, c'est un ouvert convexe. On a $L \cap B = \emptyset$ car si $y \in L$ $|f(y)| = 1 \leq \|f\|\|y\|$. Ainsi on applique Hahn-Banach géométrique et donc il existe un hyperplan affine H tel que $H \cap B = \emptyset$ et $L \subset H$.

On définit $\tilde{f}$ par : $\tilde{f}(x) = 1$ pour $x \in H$ (comprendre pourquoi on a alors définit $\tilde{f}$ sur X). Ainsi $\ker f = \overrightarrow{H}$ où $\overrightarrow{H}$ est l'hyperplan vectoriel qui dirige H. $\tilde{f}$ prolonge bien f car pour $m \in M - \ker f$ il existe $\mu \in \mathbb{R}$ tel que $m = \mu l$ avec $l \in L$.



Il reste à montrer que ce prolongement préserve la norme de f. Il faut montrer que $|\tilde{f}(y)| \leq \|f\|\|y\|$ pour $y \in X$. Pour $y \in X - \ker f$, il existe $\lambda \in \mathbb{R}$ tel que $y = \lambda h$ avec $h \in H$ et $|\tilde{f}(y)| = |\lambda|$. Or h n'est pas dans B donc $\|h\| \geq \frac{1}{\|f\|}$ c'est-à-dire $\|y\| = |\lambda|\|h\| \geq \frac{|\lambda|}{\|f\|}$ donc $|\lambda| \geq \|f\|\|y\|$ d'où $|\tilde{f}(y)| \geq \|f\|\|y\|$ c'est-à-dire $\|\tilde{f}\| = \|f\|$.

20. Théorème de Jung

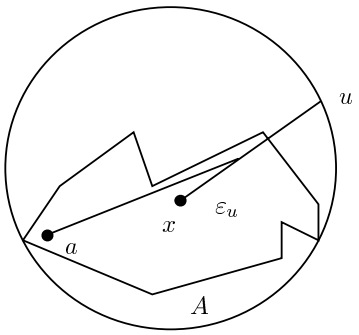
Cf : Berger T2 p.41.

Théorème 26. *Soient X un espace affine euclidien de dimension d et A un compact de X, alors A est contenu dans une boule unique de rayon minimum. En outre, si x est le centre et r le rayon de cette boule on a :*

(i) $r \leq \sqrt{\dfrac{d}{2(d+1)}} \cdot diam(A)$ *et c'est le meilleur majorant possible.*

(ii) $x \in \varepsilon(A \cap S(x,r))$ *où* $\varepsilon(B)$ *est l'enveloppe convexe de* B.

Un bout de preuve : Pour le début de la preuve cf Berger T2 p.41. Je vais donner un bout de preuve : celle qui concerne (ii). On vectorialise X en x. Soient $u \in S(x,1)$ et $\varepsilon > 0$, comme $A \subset B(x,r)$ on a $d(x,a) \leq r$ et donc il existe $a \in A$ tel que $d(x,a) \leq r < d(a, \varepsilon u)$. La deuxième inégalité est vraie sinon pour tout $a \in A$ on a $d(a, \varepsilon u) \leq r$ donc $A \subset B(\varepsilon u, r)$ et par unicité du centre de la boule cherchée $x = \varepsilon u$, c'est absurde.



Ainsi on définit une suite $(a_n)_{n\in\mathbb{N}}$ dans A par le raisonnement suivant : on prend $\varepsilon = \frac{1}{n}$ et pour chaque n il existe $a_n \in A$ tel que

$$d(x,a_n) \leq r < d(a_n, \frac{u}{n}). \tag{1}$$

Par compacité de A on extrait une sous-suite convergente, on la note encore a_n et $\lim\limits_{n\to+\infty} a_n = a$ et $d(a,x) = r$. De plus a vérifie $\langle a, u\rangle \leq 0$. En effet l'inégalité (1) donne : (on a vectorialisé en x)

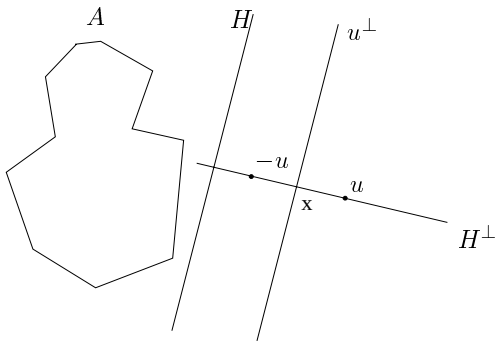
$$\begin{array}{rcccl} d(a_n,x)^2 = \|a_n\|^2 & \leq & r^2 & \leq & \|a_n\|^2 + \|\frac{u}{n}\|^2 - 2\langle a_n, \frac{u}{n}\rangle \\ 0 & \leq & r^2 - \|a_n\|^2 & \leq & \frac{1^2}{n^2} - \frac{2}{n}\langle a_n, u\rangle \end{array}$$

D'où $\langle a_n, u\rangle \leq \frac{1}{2n}$ et quand n tend vers l'infini et on a :

$$\langle a, u\rangle \leq 0 \tag{2}$$

Supposons que $x \notin \varepsilon(A \cap S(x,r))$ alors le corollaire 6 appliqué à x compact et au convexe $\varepsilon(A \cap S(x,r))$ affirme l'existence d'un hyperplan affine H séparant strictement x et $A \cap S(x,r)$. Donc H sépare strictement x et $A \cap S(x,r)$. On considère une droite vectorielle orthogonale à H, on la note $H^\perp$ et on soit $\{u, -u\} = S(x,1) \cap H^\perp$. On a $u^\perp$ qui est l'hyperplan vectoriel dirigeant H. Et $u^\perp$ sépare strictement soit u et $A \cap S(x,r)$ soit $-u$ et $A \cap S(x,r)$. Supposons qu'on soit dans le premier cas alors pour tout $a \in A, \langle a, -u\rangle \geq 0$ et cela contredit l'inégalité (2) donc $x \in \varepsilon(A \cap S(x,r))$.

Remarques :



(1) L'inégalité dans (i) est atteinte si $d(a_i, a_j) = \delta$ pour tout $i \neq j$; ce qui arrive pour un simplexe régulier.
(2) Remarquer qu'on utilise le théorème de Carathéodory (cf Berger T2 p.21).
(3) Se préparer à des questions du style : pourquoi l'enveloppe convexe est-elle convexe ? Est-ce qu'un convexe compact est toujours l'enveloppe convexe de sa frontière ? (cf Berger T2 p.23) Connaissez-vous le théorème de Krein-Milman? (Berger T 2p.47) ... Bref avoir quelques restes (ha!) des 50 premières pages de Berger T 2.

21. Espace vectoriel de dimension finie

Cf : Arnaudiès T1 p.379, Ramis T1 p.293

Définition 2. *Un k-espace vectoriel est de dimension finie s'il possède une partie génératrice de dimension finie.*

Théorème 27 (Arnaudiès T1 p.379)**.** *Soit E un k-espace vectoriel de dimension finie, L une partie libre de E et G une partie génératrice de E, alors il existe une partie base β de E (libre et génératrice) telle que $L \subset \beta \subset L \cup G$.*

Remarque : C'est le théorème de la base incomplète.
Remarque : La partie génératrice G n'est pas supposée finie (on a bien envie d'appliquer le théorème à $L = \emptyset$ et $G = E$ par exemple).

Lemme 4. *Soit E un k-espace vectoriel de dimension finie et soit A une partie génératrice de E. Il existe une partie G finie de A qui engendre E.*

Corollaire 7. *Dans un k-espace vectoriel de dimension finie, toute famille libre est finie.*

Corollaire 8. *Dans un k-espace vectoriel de dimension finie, il existe une base.*

Théorème 28 (Ramis T1 p.293)**.** *Dans un k-espace vectoriel de dimension finie E, les bases sont de même cardinal.*
On dit alors que ce cardinal est la dimension de E.

Remarque : Attention, le jury demande aux candidats de bien maîtriser les choses simples et ceci en est une. Il est donc indispensable de savoir comment on définit la notion de dimension d'un espace vectoriel. Et comme on est attendu au tournant autant préparer le virage c'est-à-dire le proposer en développement. Savoir démontrer, à partir de la définition,

- que, s'il existe une partie génératrice finie, toute partie génératrice contient une partie génératrice finie
- qu'un sous-espace d'un espace de dimension finie est de dimension finie (pas si simple, si on n'y a pas réfléchi avant...).

22. $\mathbb{F}_q^\star$ EST CYCLIQUE ET QUAND A-T-ON $\mathbb{F}_q \subset \mathbb{F}_{q'}$?

Cf : Perrin p.74 Francinou p.134

Théorème 29. *$\mathbb{F}_q^\star$ est cyclique.*

Proposition 7. *$\mathbb{F}_q$ est inclus dans $\mathbb{F}_{q'}$ si et seulement si $q = p^n, q' = p^{n'}$ et n divise n'.*

Exercice : Construire $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8$ et $\mathbb{F}_{16}$.

Remarque : C'est pas tonitruant, mais bon...
Voilà un exercice vraiment cool sur les corps finis :

Exercice : Un bateau qui comprend 31 vacanciers part pour un voyage qui dure tout le mois d'août. Le capitaine de se bateau peut inviter 6 personnes chaque soir à sa table. Il veut que chaque personne se soit rencontrer une et une seule fois à sa table. Peut-il le faire ?

Solution : Oui, mais comment ?

Dans $\mathbb{F}_5^3$ il y a 124 vecteurs non nuls et étant donné un vecteur non nul x il y a $5 - 1 = 4$ vecteurs non nuls sur la droite vectoriel engendré par x. Ainsi il y a $124/4 = 32$ droites dans $\mathbb{F}_5^3$. Par dualité il y a autant de droites que de plans dans $\mathbb{F}_5^3$. Et dans chacun de ses plans il y a $(5 \cdot 5 - 1)/4 = 6$ droites vectoriels. Si on fait la correspondance une droite = un vacancier. Pour répondre à son problème, notre cher capitaine doit inviter chaque soir (en août il y a 31 jours!) un plan différent, c'est à dire 6 droites, c'est à dire 6 vacanciers. Et chaque vacancier s'est rencontré une et une seul fois à la table du capitaine car deux droites définissent un unique plan.

23. LE RANG D'UNE DIFFÉRENTIELLE

Cf : Mneimné Éléments de géométrie p.194

Exercice :

Soient k le corps $\mathbb{R}$ ou $\mathbb{C}$ et μ l'application :

$$\begin{array}{rccc} \mu & : & M_n(k) & \longrightarrow & k^n \\ & & M & \longmapsto & (tr(M), tr(M^2), \ldots, tr(M^n)) \end{array}$$

Montrer que le rang de $d\mu(m)$ vaut le degré du polynôme minimal de M.

Solution :

On a $d\mu(M)(X) = (tr(X), 2tr(MX), \dots, ntr(M^{n-1}X))$ (la trace est une application linéaire).

On va calculer la dimension du noyau puis utiliser la formule du rang.

Le noyau de $d\mu(M)$ est l'intersection des hyperplans H_i d'équations $tr(M^iX)$.

Considérons $H = \bigcap_{i=1}^{n} H_i$ et $H^\perp = \{\varphi \in M_n(k)^\star | \varphi(H) = 0\}$. On va d'abord calculer la dimension de $H^\perp$.

On a $H^\perp = vect\left((\varphi_i : X \longrightarrow tr(M^iX))_{i=1,\dots,n}\right)$.

En effet (Avez p.103), il n'y a qu'un seul sens qui n'est pas "trop" trivial. Soit $\varphi_1, \dots, \varphi_r$ linéairement indépendant telles que $H^\perp = vect(\varphi_1, \dots, \varphi_r)$. On complète $(\varphi_1, \dots, \varphi_r)$ en une base $(\varphi_1, \dots, \varphi_r, e^\star_{r+1}, \dots, e^\star_n)$ de $M_n(k)^\star$ et soit $(f_1, \dots, f_r, e_{r+1}, \dots, e_n)$ la base antéduale de E. Ainsi si $a \in H^\perp$ alors $a = \lambda_1\varphi_1 + \dots + \lambda_r\varphi_r + \mu_{r+1}e^\star_{r+1} + \dots + \mu_n e^\star_n$. et comme $H = vect(e_{r+1}, \dots, e_n)$ on a $a(e_i) = 0$ donc $\mu_i = 0$.

Puis comme $\psi : (X, Y) \longrightarrow tr(XY)$ est une forme bilinéaire non dégénérée sur $M_n(k) \times M_n(k)$ (vérification immédiate, attention, ce n'est *pas* la forme euclidienne sur les matrices, même si le corps est $\mathbb{R}$) alors l'application

$$\begin{array}{rccc} \tilde{\psi} : & M_n(k) & \longrightarrow & M_n(k)^\star \\ & M & \longmapsto & \psi(M, \cdot) \end{array}$$

est un isomorphisme. Et si on note $F_M = vect(\varphi_i)_{i=1,\dots,n}$ alors $k[M]$ se surjecte sur F_M par $\tilde{\psi}$. Or $\tilde{\psi}$ est injective donc F_M est isomorphe à $k[M]$. Et la dimension de $k[M]$ vaut le degré du polynôme minimal de M. On conclut en utilisant $\dim A^\perp + \dim A = \dim E$ et la formule du rang c'est-à-dire $\dim H^\perp = rg(d\mu(M))$ qui vaut le degré du polynôme minimal.

Conséquence : On peut montrer que $\{M \in M_n(k) | \chi_M = (-1)^n \Pi_M\}$ (où Π_M est le polynôme minimal et χ_M est le caractéristique) est un ouvert.

En effet, le degré de χ_M est n et le degré de Π_M est le rang de $d\mu(M)$. Or $\{M | \operatorname{rg} d\mu(M) = n\}$ est un ouvert car $d\mu(M)$ est alors de rang maximal (cf le paragraphe 25.2).

24. Ellipsoïde de John

Cf : Leichtnam T 2 p.158.

Soit $\mathbb{R}^n$ muni de la norme euclidienne, on note :

- $Q = \{$ formes quadratiques sur $\mathbb{R}^n\}$
- $Q^+ = \{$ formes quadratiques positives sur $\mathbb{R}^n\}$
- $Q^{++} = \{$ formes quadratiques définies positives sur $\mathbb{R}^n\}$

Pour $q \in Q$, on note E_q l'ellipsoïde $\{x \in \mathbb{R}^n$ tel que $0 \leq q(x) \leq 1\}$. Pour $q \in Q^{++}$, on note $V(q) = \dfrac{1}{\sqrt{\operatorname{disc}(q)}}$ (=le volume de E_q).

Théorème 30. *Soit K un compact d'intérieur non vide de $\mathbb{R}^n$, alors il existe une unique forme quadratique définie positive telle que K soit inclus dans E_q et $V(q)$ soit minimal.*

Preuve : Commençons par montrer l'existence. Considérons $A = \{q \in Q^+ \text{ tel que } K \subset E_q\}$.

(1) A est non vide. En effet, comme K est compact, il est borné c'est-à-dire il existe $M > 0$ tel que $\|x\| \leq M$ pour tout $x \in K$. Alors on pose $q(x) = \dfrac{\|x\|^2}{M^2}$ et q est dans A.

(2) A est fermé dans (Q, N) où $N(q) = \sup_{\|x\|=1} |q(x)|$.

Soit $(q_n)_{n\in\mathbb{N}}$ une suite d'éléments de A qui converge vers q_∞ et q_∞ est dans Q^+ (car Q^+ est fermé dans Q). Comme on a

$$\lim_{n\to+\infty} N(q_n - q_\infty) = 0,$$

alors pour tout x dans $\mathbb{R}^n$, $q_n(x)$ tend vers $q_\infty(x)$. Or pour tout n et pour tout $x \in K$ on a $0 \leq q_n(x) \leq 1$, en passant à la limite on a : pour tout x dans K, $0 \leq q_\infty(x) \leq 1$. Ainsi q_∞ est dans A et donc A est fermé dans Q^+ qui est lui même fermé dans (Q, N), c'est-à-dire A est fermé dans Q.

(3) A est borné dans (Q, N). En effet, comme K est d'intérieur non vide alors il existe $a \in K$ et $r > 0$ tels que $\overline{B}(a, r)$ soit inclus dans K. Soit $q \in A$, pour tout x dans S, où $S = \{x \in \mathbb{R}^n \text{ tel que } \|x\| = 1\}$, $a + rx$ est dans $\overline{B}(a, r) \subset K \subset E_q$. C'est-à-dire pour tout x dans S on a $q(a + rx) \leq 1$. Par l'inégalité triangulaire (cette inégalité est vraie pour une forme quadratique positive pas nécessairement définie positive) on a pour tout $x \in S$:

$$\begin{array}{rcccl} r\sqrt{q(x)} - \sqrt{q(a)} & \leq & \sqrt{q(a+rx)} & \leq & 1 \\ \sqrt{q(x)} & \leq & \dfrac{\sqrt{q(a)}+1}{r} & \leq & \dfrac{2}{r} \text{ car } a \in K \subset E_q \end{array}$$

D'où $N(q) \leq \dfrac{4}{r^2}$ et ceci est vrai pour tout q dans A donc A est borné.

Ainsi d'après (1),(2) et (3), A est non vide, fermé et borné donc il est compact dans Q qui est un espace vectoriel de dimension finie.

(4) L'application qui, à $q \in Q$ associe $\text{disc}(q) \in \mathbb{R}$ est continue. En particulier elle est bornée sur le compact non vide A et donc elle atteint son maximum en $q_0 \in A$. On a déjà trouvé $q \in A$ tel que $q \in Q^{++}$ c'est-à-dire $\text{disc}(q) > 0$ (pour montrer que A est non vide) donc $q_0 \in Q^{++}$. Il existe donc $q_0 \in Q^{++}$ qui minimise $V(q)$ et qui vérifie $K \subset E_{q_0}$.

Montrons maintenant l'unicité.

(1) Q^{++} est un ensemble convexe.

(2) L'application qui envoie $q \in Q^{++}$ sur $V(q) \in \mathbb{R}$ est strictement convexe. En effet, soient q et q' dans Q^{++} et soient M et M' leurs matrices respectives, d'après le théorème de réduction simultanée il

existe $P \in Gl(n,\mathbb{R})$ tel que :

$$M = {}^tP \cdot \begin{pmatrix} a_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & a_n \end{pmatrix} \cdot P, M' = {}^tP \cdot \begin{pmatrix} b_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & b_n \end{pmatrix} \cdot P$$

où a_i et b_i sont strictement positifs. Alors pour $0 < t < 1$, on a

$$\begin{aligned} V(tq + (1-t)q') &= \det \left({}^tP \begin{pmatrix} ta_1 + (1-t)b_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & ta_n + (1-t)b_n \end{pmatrix} P \right)^{-1/2} \\ &= \frac{\prod_{i=1}^n (ta_i + (1-t)b_i)^{-1/2}}{|\det P|} \\ &< \frac{\prod_{i=1}^n (a_i^t b_i^{1-t})^{-1/2}}{|\det P|} \end{aligned}$$

car le logarithme est strictement concave. Donc

$$\begin{aligned} V(tq + (1-t)q') &< \frac{\left(\prod_{i=1}^n a_i^{-1/2}\right)^t \left(\prod_{i=1}^n b_i^{-1/2}\right)^{1-t}}{|\det P|} \\ &< \frac{\prod_{i=1}^n (a_i^t b_i^{1-t})^{-1/2}}{|\det P|} \\ &< \frac{\left(\prod_{i=1}^n a_i^{-1/2}\right)^t \left(\prod_{i=1}^n b_i^{-1/2}\right)^{1-t}}{|\det P|} \end{aligned}$$

par stricte concavité du logarithme. Enfin

$$\begin{aligned} V(tq + (1-t)q') &< \frac{t\prod_{i=1}^n a_i^{-1/2} + (1-t)\prod_{i=1}^n b_i^{-1/2}}{|\det P|} \\ &= tV(q) + (1-t)V(q'). \end{aligned}$$

On a utilisé la stricte concavité du logarithme c'est-à-dire $\forall x, y > 0$ et $0 < t < 1$ on a

$$\ln(tx + (1-t)y) > t \ln x + (1-t) \ln y$$

et comme l'exponentielle est une fonction croissante, on a

$$tx + (1-t)y > x^t y^{1-t}$$

(3) Une fonction strictement convexe admet au plus un minimum : en effet si $a \neq b$ sont des minima de f (on a aussi $f(a) = f(b) = \min f$) alors $f(\frac{a+b}{2}) < \frac{f(a)}{2} + \frac{f(b)}{2} = f(a)$, ce qui est absurde. Le minimum de V sur Q^{++} est donc unique.

Remarques :

(1) Le discriminant d'une forme quadratique réelle est le déterminant de sa matrice dans une base orthonormée.

(2) Pourquoi $V(q)$ est le volume de l'ellipsoïde E_q (à une constante multiplicative près)? On a :

$$\mathrm{vol}(E_q) = \int_{\mathbb{R}^n} \chi_{\{x \in \mathbb{R}^n | q(x) \leq 1\}} dx$$

On applique le théorème de réduction à la matrice A de q dans la base canonique, ainsi il existe $P \in O(n)$ et $a_i > 0$ tel que :

$$A = {}^tP \cdot \begin{pmatrix} a_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & a_n \end{pmatrix} \cdot P \text{ où } a_i > 0$$

Dans cette nouvelle base orthonormée on a :

$$\mathrm{vol}(E_q) = \int_{\mathbb{R}^n} \chi_{\{x \in \mathbb{R}^n | a_1 x_1^2 + \cdots + a_n x_n^2 \leq 1\}} dx$$

On fait le changement de variable $y_i = \sqrt{a_i} x_i$ ainsi

$$\mathrm{vol}(E_q) = \frac{1}{\prod \sqrt{a_i}} \int_{\mathbb{R}^n} \chi_{\{y \in \mathbb{R}^n | y_1^2 + \cdots + y_n^2 \leq 1\}} dy$$

c'est-à-dire

$$\mathrm{vol}(E_q) = V(q) \cdot \mathrm{vol}(S^{n-1})$$

Application : Soit G un sous-groupe compact de $Gl(n, \mathbb{R})$, alors il existe $q \in Q^{++}$ tel que G soit un sous groupe de $O(q)$.

Remarque : Savoir le faire pour un sous-groupe fini[7] par moyenne. Savoir qu'il y a une démonstration par moyenne (mesure de Haar) pour un sous-groupe compact en général.

Preuve : Soit $H \subset \mathbb{R}^n$ un compact d'intérieur non vide.

- L'application

$$\begin{array}{rccccc} f & : & G \times H & \longrightarrow & G(H) & := K \text{ est continue.} \\ & & (g,h) & \longmapsto & g(h) & \end{array}$$

[7]Les plus simples des groupes compacts sont les groupes finis.

En effet, soient (g,h) et $(g_0h_0) \in G \times H$ alors :

$$\begin{array}{rcl} \|g(h) - g_0(h_0)\| & \leq & \|g(h) - g_0(h)\| + \|g_0(h) - g_0(h_0)\| \\ & \leq & \|g - g_0\|_G \cdot \|h\| + \|g_0\|_G \cdot \ |h - h_0\| \\ & \leq & \sup\{\|g - g_0\|_G, \|h - h_0\|\}(\sup_{h\in H} \|h\| + \|g_0\|_G) \\ & \leq & Cst \cdot \sup\{\|g - g_0\|_G, \|h - h_0\|\} \end{array}$$

Où on a pris comme norme sur $G \times H$ la norme suivante :

$$\|(g,h)\|_{G\times H} = \sup\{\|g\|_G, \|h\|\}$$

- $G \times H$ est compact comme produit de deux compacts. Donc K est compact car f est continue. Et comme $Id \in G$, et H est d'intérieur non vide, K est un compact d'intérieur non vide de $\mathbb{R}^n$.
- D'après le théorème précédent il existe une unique forme quadratique définie positive q telle que $K \subset E_q$ et $V(q)$ soit minimal. Montrons que pour tout x dans $\mathbb{R}^n$ et pour tout g dans G on a $q(g(x)) = q(x)$. On aura alors G sous groupe de $O(q)$. Soit g dans G, définissons q' par $q' = q \circ g$. Alors q' est dans Q^{++} et $E_{q'} = g^{-1}(E_q)$. Comme $g^{-1}(K) = K$ (par définition de K) on a $K \subset E_q$ donc $K \subset E_{q'}$. G étant compact donc borné, on a $|detg| = 1$ (sinon $|\det(g^n)| \to +\infty$) et $V(q') = \mathrm{disc}(q \circ g)^{-1/2} = V(q)$. Par unicité de q on a $q' = q$ et donc $q \circ g = q$ c'est-à-dire G est un sous-groupe $O(q)$.

Remarques :

(1) Ce développement est très bien car on peut le mettre en analyse et en algèbre (il y a une personne qui a présenté ce théorème dans ces deux oraux et il a eu l'agreg! Qui est-ce? héhé ...). Mais il utilise beaucoup d'outils : convexité, compacité, réduction simultanée des formes quadratiques, volume, discriminant, ... Il faut évidemment bien maîtriser ces outils.
(2) Le discriminant permet de classer les formes quadratiques sur $\mathbb{F}_q$ (c'est fait dans Serre).
(3) Je n'avais pas travaillé ce développement faute de temps (j'avoue mon erreur), mais il est vraiment très beau voire même universel !! Merci à monsieur John de la part de nombreux agrégés.

25. Un peu de topologie sur les matrices

Avant propos : L'idée de ce paragraphe est de déduire de théorèmes plus ou moins connus des propriétés topologiques de certains sous-ensembles de $M_{n\times p}(k)$.

Pour parler de topologie, on suppose que les matrices ont leurs coefficients dans k avec $k = \mathbb{R}$ ou $\mathbb{C}$.

25.1. **A propos de $Gl(n,k)$.**

Proposition 8 (Mneimné-Testard Groupes de Lie classiques p.14)**.** *Le groupe linéaire $Gl(n,k)$ est un ouvert dense de $M_n(k)$.*

Preuve : L'application déterminant est continue car elle est polynomiale en les coefficients de la matrice. Et comme $Gl(n,k) = \{M \in M_n(k) | \det(M) \neq 0\}$, on en déduit que $Gl(n,k)$ est un ouvert de $M_n(k)$. Soit $M \in M_n(k)$, on pose $\lambda_0 = \min(|\lambda_i|)$ où les λ_i sont les valeurs propres de M. Ainsi $M - \lambda Id$ pour $0 < |\lambda| < \lambda_0$ est inversible (c'est la définition des valeurs propres) et $\lim_{\lambda \to 0} M - \lambda Id = M$. C'est-à-dire $Gl(n,k)$ est dense dans $M_n(k)$.

Application : Pour $A, B \in M_n(k)$, le polynôme caractéristique de AB est égal au polynôme caractéristique de BA.

Définition 3 (Cf Perrin p.96 et Gourdon algèbre p.156)**.**

- *Une dilatation peut s'écrire dans une base*
$$D(\mu) = \begin{pmatrix} 1 & & \boldsymbol{0} \\ & \ddots & \\ & & 1 \\ \boldsymbol{0} & & \mu \end{pmatrix} \text{ avec } \mu \neq 1$$
- *Une transvection peut s'écrire dans une base $T_{ij}(\lambda) = I_n + \lambda E_{ij}$ avec $\lambda \neq 1$.*

Remarque : Dans Perrin il y a une interprétation géométrique des transvections et des dilatations avec différentes définitions possibles.

Théorème 31 (Perrin p.99)**.**

- *Les transvections et les dilatations engendrent $Gl(E)$.*
- *Les transvections engendrent $Sl(E)$.*

Remarque : Perrin donne une démonstration géométrique de ce théorème, mais on peut aussi démontrer ce résultat en faisant des opérations élémentaires sur les lignes et les colonnes (c'est l'algorithme du pivot de Gauss).

Applications :

(1) $Gl(n,\mathbb{C})$ et $Sl(n,\mathbb{C})$ sont des ensembles connexes.
(2) $Gl(n,\mathbb{R})$ a deux composantes connexes : $Gl(n,\mathbb{R})^+$ et $Gl(n,\mathbb{R})^-$ (qui sont homéomorphes entre elles).

Preuve : On va démontrer 1 et 2 d'un seul coup. On va montrer que ces ensembles sont connexes par arcs. On relie $T_{ij}(\lambda)$ à l'identité en faisant tendre λ vers 0. Comme $\mathbb{C} - \{0\}$ est connexe, $Gl(n,\mathbb{C})$ et $Sl(n,\mathbb{C})$ sont connexes ($\{D(\mu) | \mu \neq 0\}$ est homéomorphe à $\mathbb{C} - \{0\}$). Par contre $\mathbb{R} - \{0\}$ a deux composantes connexes donc $Gl(n,\mathbb{R})$ a deux composantes connexes.

Remarque : On peut aussi s'intéresser au centre de $Gl(E)$ et à son groupe dérivé (Cf Perrin). A ce propos on a l'application suivante :

Application : (Gourdon algèbre p.156)

Pour $n \geq 3$, soit φ un morphisme de $Gl(n,k)$ dans un groupe commutatif G alors il existe un morphisme g de $k^\star$ dans G tel que $\varphi = g \circ \det$.

Exercice :

Montrer que $Gl(n,\mathbb{C})$ est isomorphe à $Gl(p,\mathbb{C})$ si et seulement si $n = p$.

Solution :

On va regarder un sous-groupe G fini et abélien dans $Gl(n,\mathbb{C})$. Soit M dans G alors il existe un entier p tel que $M^p = I_n$. Donc M est annulé par un polynôme à racines simples ainsi M est diagonalisable et comme G est abélien, il existe une "bonne" base qui diagonalise tous les éléments de G. Maintenant on regarde les sous-groupes de $Gl(n,\mathbb{C})$ isomorphe à $(\mathbb{Z}/2\mathbb{Z})^q$. On choisit une base qui diagonalise tous les éléments de G et pour $q > n$, $(\mathbb{Z}/2\mathbb{Z})^q$ ne s'injecte pas dans $Gl(n,\mathbb{C})$ et $(\mathbb{Z}/2\mathbb{Z})^n$ est isomorphe aux matrices qui ont des ± 1 sur la diagonale. Ainsi si $n \neq p$ alors $Gl(p,\mathbb{C})$ est $Gl(n,\mathbb{C})$ ne sont pas isomorphes.

25.2. **Le rang.**

Théorème 32. *Pour M dans $M_{n\times p}(k)$, le rang d'une matrice est la taille de la plus grande sous-matrice inversible.*

Conséquences :

(1) Le rang est localement croissant. En effet, si un mineur $r \times r$ est non nul alors ce mineur est encore non nul dans un voisinage U. Ainsi sur U le rang de la matrice est forcément supérieur à r. (On sait aussi que les matrices inversibles sont denses cf la propriété 8)

(2) Le rang de la comatrice est $n, 1$ ou 0. En effet, si M est de rang n alors M est inversible et donc la transposé de la comatrice est "presque" M^{-1} c'est-à-dire son rang est n. Si le rang de M est $n-1$, alors un de ces mineurs $(n-1)\times(n-1)$ est non nul donc $M \neq 0$. puis comme le produit ${}^cMM = 0$ on a $\operatorname{Im} M \subset \ker {}^cM$. D'où $\dim \ker {}^cM \geq n-1$ et comme ${}^cM \neq 0$, le rang de la comatrice vaut 1 (par le théorème du rang). Si le rang de M est inférieur à $n-2$ alors tous les mineurs $(n-1)\times(n-1)$ sont nuls et donc ${}^cM = 0$.

(3) L'ensemble E_p des matrices de rang inférieur à p est fermé. En effet, une matrice de rang inférieur à p a tous ces mineurs $(p+1)\times(p+1)$ nuls donc E_p est une intersection fini de fermé. Car si on fixe un mineur, l'ensemble des matrices dont ce mineur est nul est un fermé (c'est la réciproque du fermé $\{0\}$ par le déterminant qui est continu).

Théorème 33. *Soit $M \in M_{n\times p}(k)$ et soit r le rang de M alors M est équivalente à la matrice*

$$J_r = \begin{pmatrix} I_r & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} \end{pmatrix}.$$

En d'autres termes, les orbites de la relation d'équivalence des matrices sont caractérisées par leur rang.

Remarque : On peut s'intéresser à la même relation d'équivalence mais avec des matrices dont les coefficients sont des anneaux euclidiens voire principaux et le résultat est donné dans le paragraphe 4.

Conséquence : La démonstration peut se faire avec des opérations sur les lignes et les colonnes (on peut aussi la faire directement en considérant une application linéaire et en choisissant des bases adaptées). Et cette démonstration qui est basée sur le pivot de Gauss permet de voir que $Gl(n,\mathbb{R})$ est engendré par les transvections et les dilatations. Puis comme en 25.1 on en déduit des résultats de connexité de $Gl(n,\mathbb{C}),\ldots$

Exercice : [Mneimné p.41]
Soit f une application de $M_n(k)$ dans k telle que $f(AB)=f(A)f(B)$ et f non identiquement constante à 1 et à 0. Alors $f(A)=0$ si et seulement si $\det(A)=0$.

Solution :

- Si $\det(A)\neq 0$ alors A est inversible. On a $f(Id)=f(AA^{-1})=f(A)f(A^{-1})$, or $f(Id\cdot Id)=f(Id)^2$ ainsi $f(Id)=0$ ou 1. Si $f(Id)=0$ alors f est identiquement nulle ce qui est contraire aux hypothèses donc $f(Id)=1$. D'où $f(A^{-1})=f(A)^{-1}\neq 0$.
- Réciproquement, soit A une matrice de rang $r<n$, si $f(A)=0$ alors le théorème 33 affirme que A est équivalente à la matrice J_r. Et comme l'image d'une matrice inversible est non nulle il suffit de montrer que $f(J_r)=0$. On considère le produit des matrices diagonales ayant r fois le nombre 1 sur la diagonale et $n-r$ fois le nombre 0 sur la diagonale. Ainsi le produit de toutes ces matrices est la matrice nulle car $r<n$. Or $f(\mathbf{0}\cdot\mathbf{0})=f(\mathbf{0})$ c'est-à-dire $f(\mathbf{0})=0$ ou 1. Si $f(\mathbf{0})=1$ alors f vaut identiquement 1 ce qui est absurde, ainsi $f(\mathbf{0})$ vaut 0. On applique f au produit des matrices diagonales ayant r fois 1 sur sa diagonale et donc f s'annule sur une de ces matrices appelons la J_r^k. Or J_r^k est équivalente à J_r (car elles ont le même rang) c'est-à-dire il existe deux matrices inversibles P et Q tel que $J_r=PJ_r^kQ$ donc $f(J_r)=f(P)f(J_r^k)f(Q)$ et comme $f(J_r^k)=0$ on a $f(J_r)=0$ c'est-à-dire $f(A)=0$.

Exercice : [Mneimné p.41] Soit H un hyperplan de $M_n(\mathbb{R})$ alors H contient une matrice inversible.

Solution :

On part de la forme euclidienne sur les matrices c'est-à-dire $\varphi(XY)=\mathrm{tr}({}^tXY)$. Elle induit un isomorphisme (car elle est non dégénérée) entre $M_n(\mathbb{R})$ est $M_n(\mathbb{R})^\star$.

Ainsi l'hyperplan H est le noyau d'une forme linéaire c'est-à-dire il existe une matrice X telle que le noyau de l'application qui à M associe $\mathrm{tr}({}^tXM)$ soit H. On est ramené à trouver une matrice inversible telle que $\mathrm{tr}({}^tXM)=0$. Or ${}^tX=PJ_rQ$ où r est le rang de X d'après le théorème 33. On cherche M telle que $\mathrm{tr}(J_rPMQ)=0$ il suffit de prendre pour PMQ la matrice de la permutation $(1,2,\ldots,r)$ car $r<n$.