Développements d'algèbre pour l'agrégation

Brice Loustau

Table des matières

Correspondance leçons ↔ développements

Leçons	Développements
101 Groupe opérant sur un ensemble. Exemples et applications.	**AL02** Sous-groupes compacts du groupe linéaire **AL10** Théorème de Frobenius-Zolotarev **AL17** Groupes finis de déplacements de l'espace **AL18** Théorèmes de Sylow **AL22** Action du groupe modulaire sur le demi-plan de Poincaré **AL24** Pavage du plan **AL25** Décomposition de Bruhat
102 Sous-groupes discrets de $\mathbb{R}^n$. Réseaux. Exemples.	(**AL12** Entiers de Gauss et théorème des deux carrés) (**AL22** Action du groupe modulaire sur le demi-plan de Poincaré) **AL24** Pavage du plan
103 Exemples de sous-groupes distingués et de groupes quotients. Applications.	**AL04** Théorème de Lie-Kolchin **AL10** Théorème de Frobenius-Zolotarev **AL18** Théorèmes de Sylow **AL22** Action du groupe modulaire sur le demi-plan de Poincaré **AL23** Groupes d'ordre 8 (**AL24** Pavage du plan)
104 Groupes finis. Exemples et applications.	**AL04** Théorème de Lie-Kolchin **AL10** Théorème de Frobenius-Zolotarev **AL17** Groupes finis de déplacements de l'espace **AL18** Théorèmes de Sylow **AL19** Théorème de Burnside **AL20** Théorème de Carlitz **AL22** Action du groupe modulaire sur le demi-plan de Poincaré **AL23** Groupes d'ordre 8
105 Groupe des permutations d'un ensemble fini. Applications.	**AL10** Théorème de Frobenius-Zolotarev (**AL14** Matrices bistochastiques)

	AL17 Groupes finis de déplacements de l'espace **AL18** Théorèmes de Sylow **AL25** Décomposition de Bruhat
106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.	**AL02** Sous-groupes compacts du groupe linéaire **AL04** Théorème de Lie-Kolchin **AL10** Théorème de Frobenius-Zolotarev **AL19** Théorème de Burnside **AL25** Décomposition de Bruhat **AN07** Théorème de Cartan-von Neumann **AL26** Décomposition polaire
107 Sous-groupes finis de $\mathrm{O}(2,\mathbb{R})$, de $\mathrm{O}(3,\mathbb{R})$. Applications.	**AL17** Groupes finis de déplacements de l'espace **AL24** Pavage du plan
108 Exemples de parties génératrices d'un groupe.	**AL10** Théorème de Frobenius-Zolotarev **AL20** Théorème de Carlitz **AL22** Action du groupe modulaire sur le demi-plan de Poincaré (**AL23** Groupes d'ordre 8) **AL24** Pavage du plan
109 Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.	(**AL01** Facteurs invariants) (**AL07** Théorème de Gauss (polygones réguliers constructibles)) **AL10** Théorème de Frobenius-Zolotarev (**AL13** Théorème de Chevalley-Warning)
110 Nombres premiers. Applications.	**AL07** Théorème de Gauss (polygones réguliers constructibles) **AL10** Théorème de Frobenius-Zolotarev **AL12** Entiers de Gauss et théorème des deux carrés (**AL13** Théorème de Chevalley-Warning)
111 Exemples d'applications des idéaux d'un anneau commutatif unitaire.	**AL01** Facteurs invariants **AL12** Entiers de Gauss et théorème des deux carrés **AL20** Théorème de Carlitz **AL21** Décomposition de Dunford effective
146 Anneaux principaux.	**AL01** Facteurs invariants (**AL12** Entiers de Gauss et théorème des deux carrés)

	(**AL21** Décomposition de Dunford effective)
112 Corps finis. Applications.	(**AL07** Théorème de Gauss (polygones réguliers constructibles)) **AL10** Théorème de Frobenius-Zolotarev **AL13** Théorème de Chevalley-Warning **AL16** Dénombrement des polynômes irréductibles sur un corps fini
113 Groupe des nombres complexes de module 1. Applications.	(**AL07** Théorème de Gauss (polygones réguliers constructibles)) (**AN16** Suites équiréparties)
114 Équations diophantiennes du premier degré $ax + by = c$. Autres exemples d'équations diophantiennes.	**AL12** Entiers de Gauss et théorème des deux carrés **AL27** Dénombrement des solutions d'une équation diophantienne
115 Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.	**AL09** Automorphismes de $k(X)$ **AL27** Dénombrement des solutions d'une équation diophantienne
116 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.	(**AL07** Théorème de Gauss (polygones réguliers constructibles)) **AL09** Automorphismes de $k(X)$ **AL15** Théorème de l'élément primitif **AL16** Dénombrement des polynômes irréductibles sur un corps fini (**AL21** Décomposition de Dunford effective)
117 Algèbre des polynômes à n indéterminées ($n \geqslant 2$). Polynômes symétriques. Applications.	**AL06** Prolongement des identités algébriques **AL13** Théorème de Chevalley-Warning
118 Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.	**AL03** Théorème *abc* pour les polynômes **AL05** Ellipse de Steiner (**AL07** Théorème de Gauss (polygones réguliers constructibles)) **AL11** Comptage de racines et forme quadratique (**AL15** Théorème de l'élément primitif) (**AL16** Dénombrement des polynômes irréductibles sur un corps fini) **AN09** Théorème de d'Alembert-Gauss (**AN14** Méthode de quadrature de Gauss) (**AN17** Méthode de Newton)
	((**AL01** Facteurs invariants))
120 Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.	

	((**AL07** Théorème de Gauss (polygones réguliers constructibles))) **AL15** Théorème de l'élément primitif (**AL16** Dénombrement des polynômes irréductibles sur un corps fini) (**AN01** Sous-espaces stables par translations)
121 Matrices équivalentes.Matrices semblables. Applications.	**AL01** Facteurs invariants **AL02** Sous-groupes compacts du groupe linéaire **AL04** Théorème de Lie-Kolchin
122 Opérations élémentaires sur les lignes et les colonnes d'une matrice. Résolution d'un système d'équations linéaires. Exemples et applications.	**AL01** Facteurs invariants (**AL14** Matrices bistochastiques) **AL25** Décomposition de Bruhat
123 Déterminant. Exemples et applications.	**AL01** Facteurs invariants (**AL06** Prolongement des identités algébriques) **AL10** Théorème de Frobenius-Zolotarev (**AL28** Théorèmes de Perron-Frobenius) (**AN01** Sous-espaces stables par translations)
124 Réduction d'un endomorphisme en dimension finie. Applications.	**AL04** Théorème de Lie-Kolchin **AL21** Décomposition de Dunford effective (**AL28** Théorèmes de Perron-Frobenius) ((**AN25** Théorème de stabilité de Liapounov))
125 Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.	**AL04** Théorème de Lie-Kolchin (**AL21** Décomposition de Dunford effective) ((**AL28** Théorèmes de Perron-Frobenius)) (**AN01** Sous-espaces stables par translations)
126 Endomorphismes diagonalisables.	(**AL04** Théorème de Lie-Kolchin) (**AL06** Prolongement des identités algébriques) **AL21** Décomposition de Dunford effective (**AN11** Théorème de Gershgörin)
127 Exponentielle de matrices. Applications.	**AN07** Théorème de Cartan-von Neumann **AN25** Théorème de stabilité de Liapounov
128 Endomorphismes nilpotents.	**AL19** Théorème de Burnside **AL21** Décomposition de Dunford effective
129 Polynômes d'endomorphismes. Polynômes annulateurs. Applications.	(**AL06** Prolongement des identités algébriques) **AL19** Théorème de Burnside

	AL21 Décomposition de Dunford effective (**AL28** Théorèmes de Perron-Frobenius) (**AN11** Théorème de Gershgörin)
130 Exemples de décompositions remarquables dans le groupe linéaire. Applications.	**AL25** Décomposition de Bruhat **AL26** Décomposition polaire
131 Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.	((**AL02** Sous-groupes compacts du groupe linéaire)) **AL11** Comptage de racines et forme quadratique **AN25** Théorème de stabilité de Liapounov
132 Formes linéaires et hyperplans en dimension finie. Exemples et applications.	**AL08** Enveloppe convexe de O(n) (**AL11** Comptage de racines et forme quadratique) (**AL15** Théorème de l'élément primitif) **AN01** Sous-espaces stables par translations
133 Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie.	(**AL02** Sous-groupes compacts du groupe linéaire) **AL08** Enveloppe convexe de O(n) **AL17** Groupes finis de déplacements de l'espace **AL26** Décomposition polaire (**AL24** Pavage du plan)
134 Endomorphismes remarquables d'un espace vectoriel hermitien de dimension finie.	**AL26** Décomposition polaire
135 Isométries d'un espace affine euclidien de dimension finie. Formes réduites. Applications.	**AL17** Groupes finis de déplacements de l'espace **AL24** Pavage du plan
136 Coniques. Applications.	**AL05** Ellipse de Steiner
137 Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.	(**AL02** Sous-groupes compacts du groupe linéaire) **AL08** Enveloppe convexe de O(n) **AL14** Matrices bistochastiques
138 Homographies de la droite complexe. Applications.	(**AL22** Action du groupe modulaire sur le demi-plan de Poincaré)
139 Applications des nombres complexes à la géométrie.	**AL05** Ellipse de Steiner (**AL07** Théorème de Gauss (polygones réguliers constructibles)) **AL22** Action du groupe modulaire sur le demi-plan de Poincaré (**AL24** Pavage du plan)
140 Angles : Définitions et utilisation en géométrie.	**AL05** Ellipse de Steiner (**AL07** Théorème de Gauss (polygones réguliers constructibles))

	(**AL24** Pavage du plan)
141 Utilisation des groupes en géométrie.	(**AL07** Théorème de Gauss (polygones réguliers constructibles)) **AL22** Action du groupe modulaire sur le demi-plan de Poincaré **AL24** Pavage du plan
142 Exemples de propriétés projectives et d'utilisation d'éléments à l'infini.	(**AL22** Action du groupe modulaire sur le demi-plan de Poincaré)
143 Constructions à la règle et au compas.	**AL07** Théorème de Gauss (polygones réguliers constructibles)
147 Applications affines.	**AL24** Pavage du plan
144 Problèmes d'angles et de distances en dimension 2 ou 3.	**AL05** Ellipse de Steiner **AL07** Théorème de Gauss (polygones réguliers constructibles) (**AL24** Pavage du plan)
145 Méthodes combinatoires, problèmes de dénombrement.	**AL11** Comptage de racines et forme quadratique **AL16** Dénombrement des polynômes irréductibles sur un corps fini **AL27** Dénombrement des solutions d'une équation diophantienne **AN02** Dénombrement des partitions d'un ensemble fini
148 Groupe orthogonal d'une forme quadratique.	(**AL02** Sous-groupes compacts du groupe linéaire) (**AL08** Enveloppe convexe de $\mathrm{O}(n)$)
149 ? Groupes de petits cardinaux.	**AL17** Groupes finis de déplacements de l'espace **AL20** Théorème de Carlitz **AL23** Groupes d'ordre 8

1 Facteurs invariants d'une matrice

THÉORÈME. *Soit A un anneau principal et $M \in \mathcal{M}_{m\times n}(A)$ (où m, $n \in \mathbb{N}^*$). Il existe alors une suite $(d_1, ..., d_s)$ d'éléments de A vérifiant $d_1|...|d_s$ tels que M soit équivalente à la matrice diagonale de coefficients diagonaux $(d_1, ..., d_s)$. Les d_i sont uniques à inversibles près, ils sont appelés facteurs invariants de la matrice M.*

Preuve.
Nous allons faire une preuve algorithmique dans le cas où A est un anneau euclidien. Cette preuve se généralise de manière non constructive dans le cas où A est seulement supposé principal. On note φ le stathme de A.

Étape 0. Si M est la matrice nulle, l'algorithme est terminé.

Étape 1. Sinon, ramener le coefficient non nul de stathme minimale en haut à gauche de la matrice par une permutation de ligne et de colonne.

Étape 2 : Traitement de la première colonne. On commence par m_{21} ($i \leftarrow 2$).
a) On effectue la division euclidienne de m_{i1} par m_{11} : $m_{i1} = qm_{11} + r$ avec $r = 0$ ou $\varphi(r) < \varphi(m_{11})$. On soustrait q fois la ligne L_1 à la ligne L_i.
b) Si $r \neq 0$, on échange les lignes L_1 et L_i et on retourne en 2.a).
c) Si $r = 0$ et $i < m$, on passe à la ligne suivante ($i \leftarrow i + 1$) et on recommence en 2.a).
d) Si $r = 0$ et $i = m$, on passe à l'étape 3.

Étape 3 : Traitement de la première ligne. À ce stade de l'algorithme, la première colonne est nulle à l'exception du premier coefficient.

On commence par m_{12} ($j \leftarrow 2$).
a) On effectue la division euclidienne de m_{1j} par m_{11} : $m_{1j} = qm_{11} + r$ avec $r = 0$ ou $\varphi(r) < \varphi(m_{11})$. On soustrait q fois la colonne C_1 à la colonne C_j.
b) Si $r \neq 0$, on échange les colonnes C_1 et C_j et on retourne en 2.
c) Si $r = 0$ et $j < n$, on passe à la colonne suivante ($j \leftarrow j + 1$) et on recommence en 3.a).
d) Si $r = 0$ et $j = n$, on passe à l'étape 4.

Étape 4. À ce stade de l'algorithme, la première colonne et la première ligne sont nulles à l'exception du premier coefficient. S'il existe m_{ij} tel que m_{11} ne divise pas m_{ij} (avec i, $j \geqslant 2$), on ajoute la colonne C_j à la colonne C_1 et on retourne à l'étape 2. Sinon, on retourne à l'étape 0. avec la matrice extraite $(m_{ij})_{2\leqslant i,j}$.

L'algorithme se termine grâce à la décroissance de $\varphi(m_{11})$. Cette décroissance est stricte à chaque « retour en arrière ».

Montrons maintenant l'unicité, à inversibles près, de la suite $(d_1, ..., d_s)$. Pour une matrice $U \in \mathcal{M}_{m\times n}(A)$, on note $\Lambda_j(U) = \text{pgcd}\{\Delta_j, \Delta_j \text{ mineur de taille } j \text{ de U}\}$. Dans le cas où U est diagonale, on a $\Lambda_j(U) = d_1...d_j$, les idéaux (d_j) sont donc uniquement déterminés par les idéaux (Λ_j). Ils nous suffit donc de montrer que deux matrices équivalentes U et U' ont les

mêmes idéaux (Λ_j).

Supposons d'abord que $U = PU'$ avec $P \in \mathrm{GL}_m(A)$. Les lignes de U sont combinaisons linéaires des lignes de U'. Par multilinéarité du déterminant, un mineur de taille j de U est combinaison linéaire de mineurs de taille j de U', si bien que $(\Lambda_j(U)) \subset (\Lambda_j(U'))$. Comme on a aussi $U' = P^{-1}U$, on obtient de même $(\Lambda_j(U')) \subset (\Lambda_j(U))$, si bien que $(\Lambda_j(U)) = (\Lambda_j(U'))$. On montre de la même manière que si $U = U'Q$ avec $Q \in \mathrm{GL}_n(A)$, on a $(\Lambda_j(U')) = (\Lambda_j(U))$. On déduit de ces deux résultats que si $U = PU'Q$, alors $(\Lambda_j(U')) = (\Lambda_j(U))$, ce qu'il fallait.

□

Corollaire (Théorème de la base adaptée)**.** *Soit A un anneau principal et M un A-module libre de rang n. Si N est un sous-module de M, il existe une base $(e_1, ..., e_n)$ de M et des scalaires non nuls d_1, ..., d_s, uniques à inversibles près, vérifiant $d_1|...|d_s$ et tels que la famille $(d_1e_1, ..., d_se_s)$ soit une base de N.*

Preuve.
On admet ici qu'un sous-module d'un module libre de rang fini est également libre de rang fini.

Soit donc $(v_1, ..., v_m)$ une base de N et $(u_1, ..., u_n)$ une base de M. On écrit U la matrice dans les bases (v_i) et (u_i) de l'injection canonique de N dans M.

D'après le théorème précédent, cette matrice est équivalente à une matrice diagonale U', de coefficients diagonaux non nuls d_1, ..., d_s, tels que $d_1|...|d_s$.

Cela signifie précisément qu'il existe une base $(e_1, ..., e_n)$ de M et une base $(f_1, ..., f_m)$ de N telles que $\mathrm{id}(f_i) = d_ie_i$ pour $i \leqslant s$ et $\mathrm{id}(f_i) = 0$ pour $i > s$. On voit tout de suite que l'on a $s = n$, car cette dernière éventualité est exclue.

Le théorème précédent donne également l'unicité des d_i, à inversibles près.

□

Corollaire (Théorème de structure)**.** *Soit M un module de type fini sur un anneau principal A. Il existe un entier $n \in \mathbb{N}$ (appelé rang de M) et une suite de scalaires non nuls $d_1|...|d_s$, uniques à inversibles près (appelés facteurs invariants de M), tels que $M \simeq A^n \oplus A/(d_1) \oplus ... \oplus A/(d_s)$.*

Preuve.
Le module M étant de type fini, on dispose d'un morphisme surjectif $\varphi : A^m \to M$ (où $m \in \mathbb{N}$).

D'après le théorème précédent, il existe une base $(e_1, ..., e_m)$ de A^m et une suite de scalaires non nuls $d_1|...|d_s$ uniques à inversibles près, tels que $(d_1e_1, ..., d_se_s)$ soit une base de $\mathrm{Ker}\varphi$.

On a alors $M \simeq A^m/\mathrm{Ker}\varphi$ soit $M \simeq A^m/\bigoplus d_ie_i$ et par une identification classique $M \simeq A^n \oplus \bigoplus d_ie_i$, où $n = m - s$. L'unicité découle du théorème précédent.

□

Leçons possibles
109 Anneaux Z/nZ. Applications.
111 Exemples d'applications des idéaux d'un anneau commutatif unitaire.
122 Opérations élémentaires sur les lignes et les colonnes d'une matrice. Résolution d'un système d'équations linéaires. Exemples et applications.
146 Anneaux principaux.
121 Matrices équivalentes. Matrices semblables. Applications.

Références
[BMP05] pp. 285 et suivantes.

2 Sous-groupes compacts de $\mathbf{GL}_n(\mathbb{R})$

THÉORÈME. *Tout sous-groupe compact de $GL_n(\mathbb{R})$ est conjugué à un sous-groupe de $O_n(\mathbb{R})$.*

En particulier, $\mathrm{O}_n(\mathbb{R})$ est un sous-groupe compact maximal de $\mathrm{GL}_n(\mathbb{R})$.

Lemme. *Soient E un espace vectoriel réel de dimension finie, K un convexe compact de E et H un sous-groupe compact de $GL(E)$. Si K est stable par tous les éléments de H, alors il existe un point $a \in K$ fixé par tous les éléments de H.*

Preuve.
Soit $\|.\|$ une norme euclidienne sur E et pour $x \in E$, posons $N(x) = \sup_{u\in H} \|u(x)\| = \max_{u\in H} \|u(x)\|$ (la borne supérieure est atteinte car H est compact pour la norme induite par $\|.\|$).

N est une norme sur E. En effet,
– Si $N(x) = 0$, on a en particulier $\|\mathrm{id}_E(x)\| = 0$ d'où $x = 0$.
– Il est clair que $N(\lambda x) = \lambda N(x)$ pour $\lambda \in \mathbb{R}$.
– $N(x+y) = \max_{u\in H} \|u(x+y)\| \leqslant \max_{u\in H}(\|u(x)\|+\|u(y)\|) \leqslant \max_{u\in H} \|u(x)\|+\max_{u\in H} \|u(y)\|$ soit $N(x + y) \leqslant N(x) + N(y)$.

De plus, N vérifie la propriété suivante : pour tout $v \in H$, $N(v(x)) = N(x)$ (c'est clair car $u \mapsto u \circ v$ est une permutation de H). Enfin, N est une norme strictement convexe. Montrons-le :

Soient $x, y \in E$ tels que $N(x+y) = N(x)+N(y)$. Soit $u_0 \in H$ tel que $N(x+y) = \|u_0(x+y)\|$. Des inégalités

$$N(x + y) = \|u_0(x) + u_0(y)\| \leqslant \|u_0(x)\| + \|u_0(y)\| \leqslant N(x) + N(y) = N(x + y),$$

on déduit que $\|u_0(x) + u_0(y)\| = \|u_0(x)\| + \|u_0(y)\|$, si bien que $u_0(x)$ et $u_0(y)$ sont positivement liés (une norme euclidienne étant strictement convexe). u_0 étant linéaire et inversible, cela entraîne de même que x et y sont positivement liés.

Il s'ensuit qu'il existe un unique point a de norme N minimale sur le convexe compact K (la compacité de K donne l'existence, la convexité de K et la stricte convexité de la norme l'unicité : si deux points a_1, a_2 distincts dans K sont de norme minimale, le milieu du segment $[a_1, a_2]$ est encore dans K et de norme strictement inférieure).

Si $v \in H$, $v(a) \in K$ et $N(v(a)) = N(a)$ donc $v(a) = a$: le point a est fixé par tous les éléments de H.

□

Preuve du théorème.
Soit G un sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$. Notons E l'espace des matrices symétriques

carrées d'ordre n. L'application $\rho : \begin{array}{ccc} G & \to & \mathrm{GL}(E) \\ A & \mapsto & \rho_A \end{array}$ définie par $\rho_A(S) = {}^tASA$ est un morphisme de groupes topologiques. Le groupe $H = \rho(G)$ est donc un sous-groupe compact de $\mathrm{GL}(E)$.

L'ensemble $\mathcal{E} = \{{}^tMM, M \in G\}$ est un compact de E, son enveloppe convexe K est donc compacte d'après le théorème de Carathéodory. $\mathcal{E}$ étant inclus dans l'ensemble convexe $\mathrm{S}_n^{++}(\mathbb{R})$ des matrices symétriques définies positives, on a encore $K \subset \mathrm{S}_n^{++}(\mathbb{R})$.

Il est clair que les éléments de H laissent K stable : $\rho_A({}^tMM) = {}^t(MA)(MA)$ est élément de $\mathcal{E}$ si $M \in G$, le résultat s'ensuit par linéarité. Nous pouvons donc appliquer le lemme : il existe une matrice symétrique définie positive S qui est fixée par tous les éléments de H, autrement dit telle que ${}^tASA = S$ pour toute matrice A de G. Il est équivalent de dire que G est contenu dans le groupe orthogonal de la forme quadratique associée à S, ou encore que G est conjugué à un sous-groupe de $\mathrm{O}_n(\mathbb{R})$ (d'après le théorème de réduction des formes quadratiques).

□

Leçons possibles
101 Groupe opérant sur un ensemble. Exemples et applications.
106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications.
121 Matrices équivalentes.Matrices semblables. Applications.
(**137** Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.)
148 Groupe orthogonal d'une forme quadratique.
133 Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie.

Références
[Ale99] pp. 59-60.

3 Théorème *abc* pour les polynômes

Soit $f(t)$ un polynôme à une indéterminée à coefficients dans un corps k de caractéristique 0. On note $n_0(f)$ le nombre de racines distinctes de f dans une clôture algébrique de k.

THÉORÈME (MASON-STOTHERS). *Soient $a(t)$, $b(t)$, $c(t)$ des polynômes non constants et premiers entre eux tels que $a+b=c$. Alors* $\max\{d^\circ(a), d^\circ(b), d^\circ(c)\} \leqslant n_0(abc) - 1$.

Preuve.
Commençons par remarquer que les polynômes a, b et c sont deux à deux premiers entre eux en vertu de l'identité $a+b=c$.

On écrit que $a'c - ac' = a'(a+b) - a(a'+b') = a'b - ab'$. Le polynôme $a'b - ab'$ n'est pas nul, car sinon on aurait $a|a'$ (a étant premier avec b), ce qui est exclu si a n'est pas constant. Le pgcd $a \wedge a'$ de a et a' divise $a'b - ab'$, ainsi que $b \wedge b'$. Il en est de même de $c \wedge c'$, en vertu de l'égalité précédente.

Les polynômes a, b et c étant premiers entre eux, il en est de même des polynômes $a \wedge a'$, $b \wedge b'$ et $c \wedge c'$. Leur produit divise donc $a'b - ab'$, on en déduit que

$$d^\circ(a \wedge a') + d^\circ(b \wedge b') + d^\circ(c \wedge c') \leqslant d^\circ(a'b - ab') \leqslant d^\circ(a) + d^\circ(b) - 1.$$

Pour un polynôme $f(t)$, on a $d^\circ(f \wedge f') = d^\circ(f) - n_0(f)$, car la multiplicité dans f' d'une racine α de f est $m(\alpha) - 1$, où $m(\alpha)$ est la multiplicité de α dans f. En reportant dans l'inégalité précédente, on obtient $d^\circ(c) \leqslant n_0(a) + n_0(b) + n_0(c) - 1$.

Les polynômes a, b et c étant non constants et premiers entre eux, on a $n_0(abc) = n_0(a) + n_0(b) + n_0(c)$, si bien que l'inégalité se réécrit $d^\circ(c) \leqslant n_0(abc) - 1$.

Les positions de a, b et c étant essentiellement symétriques, la même inégalité est satisfaite par $d^\circ(a)$ et $d^\circ(b)$, et le théorème est montré.

□

Corollaire (Théorème de FERMAT pour les polynômes). *Soient $x(t)$, $y(t)$ et $z(t)$ des polynômes non constants et non associés tels que $x(t)^n + y(t)^n = z(t)^n$ (où $n \in \mathbb{N}$). Alors $n \leqslant 2$.*

Preuve.
Quitte à diviser $x(t)$, $y(t)$ et $z(t)$ par leur pgcd, on peut les supposer premiers entre eux. Les polynômes $x(t)^n$, $y(t)^n$ et $z(t)^n$ sont donc premiers entre eux, et on peut appliquer le théorème précédent : $d^\circ(x^n) \leqslant n_0(x^n y^n z^n) - 1$, avec des inégalités analogues pour y et z.

En remarquant que $d^\circ(x^n) = nd^\circ(x)$ et $n_0(x^n y^n z^n) = n_0(xyz) = n_0(x) + n_0(y) + n_0(z)$ d'où $n_0(x^n y^n z^n) \leqslant d^\circ(x) + d^\circ(y) + d^\circ(z)$, on déduit de l'inégalité précédente que

$nd^\circ(x) \leqslant d^\circ(x) + d^\circ(y) + d^\circ(z) - 1$. En sommant avec les inégalités similaires obtenues pour y et z, il vient $n(d^\circ(x) + d^\circ(y) + d^\circ(z)) \leqslant 3(d^\circ(x) + d^\circ(y) + d^\circ(z)) - 3$. Ceci n'est possible que si $n \leqslant 2$. □

On peut citer comme autre application du théorème *abc* le résultat suivant, que je ne démontre pas ici (cf. [Lan04] ex. 13 p.225) :

Corollaire (Théorème de Davenport)**.** *Soient f et g des polynômes non constants tels que $f^3 \neq g^2$. Alors $d^\circ(f^3 - g^2) \geqslant d^\circ(f)/2 - 1$.*

Leçons possibles
118 Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.

Références
[Lan04] pp. 201 et suivantes.

4 Théorème de Lie-Kolchin

Théorème (Lie-Kolchin). *On note $\mathcal{B}$ le sous-groupe des matrices triangulaires supérieures inversibles de $GL_n(\mathbb{C})$. Le théorème est le suivant :*
Si G est un sous-groupe connexe et résoluble de $GL_n(\mathbb{C})$, alors G est conjugué à un sous-groupe de $\mathcal{B}$ (autrement dit, les matrices de G sont simultanément trigonalisables).

Preuve.
On raisonne par récurrence sur n. Le cas $n = 1$ est trivial. Supposons maintenant le résultat démontré pour les espaces de dimension $< n$ (pour un certain $n \geqslant 2$), et soit G un groupe connexe résoluble de $\mathrm{GL}_n(\mathbb{C})$.

S'il existe un sous-espace strict et non trivial V de $\mathbb{C}^n$ stable sous l'action de G, le résultat s'ensuit facilement par récurrence. En effet, soit W un supplémentaire de V de sorte que $\mathbb{C}^n = V \oplus W$. Dans une base convenable, tout élément $g \in G$ a une matrice de la forme $\left[\begin{array}{c|c} g_1 & * \\ \hline 0 & g_2 \end{array}\right]$. On vérifie sans problème, en faisant un produit par blocs, que les applications $g \mapsto g_1$ et $g \mapsto g_2$ sont des morphismes de groupes, ils sont de plus évidemment continus (ce sont des projections). Le groupe $G_1 = \{g_1, g \in G\}$ (resp. $G_2 = \{g_2, g \in G\}$) est donc résoluble en tant qu'image d'un groupe résoluble par un morphisme de groupes, et il est connexe comme image continue d'un connexe. On peut donc appliquer l'hypothèse de récurrence à G_1 (resp. G_2) : il existe une matrice carrée inversible p_1 (resp. p_2), de la dimension qu'il faut, telle que toutes les matrices $p_1^{-1} g_1 p_1$ (resp. $p_2^{-1} g_2 p_2$) soient triangulaires supérieures. Il suffit alors d'appliquer la matrice de changement de base $p = \left[\begin{array}{c|c} p_1 & * \\ \hline 0 & p_2 \end{array}\right]$ aux éléments de g pour obtenir le résultat voulu.

Maintenant s'il n'existe pas de tel sous-espace V, on dit que G est irréductible (sur $\mathbb{C}^n$). Nous allons montrer qu'un sous-groupe connexe, résoluble et irréductible de $\mathrm{GL}_n(\mathbb{C})$ est commutatif, ce qui est un résultat intéressant en soi. Mais constatons tout de suite que cela permet de conclure : on sait que les matrices d'une partie commutative de $\mathrm{GL}_n(\mathbb{C})$ sont simultanément trigonalisables. On peut rappeler rapidement l'argument : par récurrence sur leur dimension, des matrices qui commutent ont un vecteur propre commun, et on conclue de nouveau par récurrence sur la dimension de l'espace.

On considère donc dorénavant un sous-groupe connexe, résoluble et irréductible G de $\mathrm{GL}_n(\mathbb{C})$. Notons m le plus petit des entiers k tels que le k-ème groupe dérivé $\mathrm{D}^k(G)$ soit réduit au groupe trivial $\{I_n\}$ (ce nombre existe par définition de la résolubilité de G). On raisonne par l'absurde et on suppose que G n'est pas commutatif, ce qui revient à dire que $m > 1$. Posons $H = \mathrm{D}^{m-1}(G)$, nous allons montrer que $H = \{I_n\}$, ce qui constituera la contradiction.

Montrons d'abord que les matrices de H sont simultanément diagonalisables. Soit V le sous-espace de $\mathbb{C}^n$ des vecteurs propres communs à tous les éléments de H, il s'agit donc de montrer que $V = \mathbb{C}^n$. Par irréductibilité de G, il suffit de montrer que V est non trivial et

stable par G. Pour le premier point, remarquons que H est commutatif : $\mathrm{D}(H) = \{I_n\}$. Il existe donc un vecteur propre commun à tous les éléments de H, ce qui assure que V n'est pas réduit à $\{0\}$. Et le second point : soit $g \in G$ et $v \in V$, on veut montrer que $g(v) \in V$, c'est-à-dire que $g(v)$ est un vecteur propre de h pour tout $h \in H$. Pour cela on écrit que $h(g(v)) = g((g^{-1}hg)(v))$. H étant distingué dans G, $g^{-1}hg$ est un élément de H si bien qu'il existe un scalaire λ tel que $(g^{-1}hg)(v) = \lambda v$. Il s'ensuit que $h(g(v)) = \lambda g(v)$, $g(v)$ est donc bien élément de V.

Par suite, on montre que $H \subset \mathrm{Z}_G$, le centre de G. Soit $h \in H$, il s'agit de prouver que $ghg^{-1} = h$ pour tout $g \in G$. On introduit pour cela $\varphi : G \to H$, $g \mapsto ghg^{-1}$. Les matrices de $\varphi(H)$ sont simultanément diagonalisables et ont les mêmes valeurs propres (celles de h), elles sont donc en nombre fini. Par ailleurs, H est connexe par dérivation d'un groupe connexe et φ est continue, $\varphi(H)$ est donc connexe. On en déduit que $\varphi(H)$ est réduit à au plus un élément, puis $\varphi(H) = \{\varphi(I_n)\} = \{h\}$, ce qu'il fallait.

Il s'ensuit facilement que les éléments de H sont des homothéties. En effet, soit $h \in H$ et λ une valeur propre de h, alors le sous-espace propre associé est non trivial et stable par G (car $H \subset \mathrm{Z}_G$), c'est donc $\mathbb{C}^n$ en entier, ce qui prouve que h est l'homothétie de rapport λ. De plus, $H \subset \mathrm{D}(G) \subset \mathrm{SL}_n(\mathbb{C})$ (on utilise ici que $m > 1$), donc $\det(h) = \lambda^n = 1$. On en déduit que H est fini (ses éléments sont des homothéties dont les rapports sont des racines n-èmes de l'unité), et comme H est connexe, il est réduit à $\{I_n\}$, ce qui achève la démonstration.

□

Leçons possibles
103 Exemples de sous-groupes distingués et de groupes quotients. Applications.
106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.
121 Matrices équivalentes. Matrices semblables. Applications.
124 Réduction d'un endomorphisme en dimension finie. Applications.
125 Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.

Références
[Pit06] pp. 2-3.
chambi algèbre corporelle

5 Ellipse de Steiner

On admet les deux propriétés suivantes vérifiée par une ellipse $\mathcal{E}$ de foyers F et F' dans un plan euclidien :
- La tangente en un point M de $\mathcal{E}$ est la bissectrice extérieure de l'angle $\widehat{F'MF}$.
- Étant donné un point M de l'ellipse et un point P à l'extérieur de $\mathcal{E}$ tel que la droite (PM) soit tangente à l'ellipse en M, l'autre tangente à l'ellipse passant par P est déterminée par l'égalité des angles $(\overrightarrow{PM}, \overrightarrow{PF'})$ et $(\overrightarrow{PF}, \overrightarrow{PM'})$ (où M' est le point de tangence). Il s'agit du lemme de Poncelet.

Évidemment il faudrait faire un dessin.

On admet aussi le théorème de Gauss-Lucas : si P est un polynôme à coefficients dans $\mathbb{C}$, les racines de P' sont barycentres des racines de P (dans le plan complexe).

Théorème. *Soit P un polynôme de degré 3 à coefficients dans $\mathbb{C}$ dont les racines z_1, z_2, z_3 sont distinctes. Alors les racines w_1 et w_2 de P' sont les foyers d'une ellipse $\mathcal{E}$ inscrite dans le triangle de sommets z_1, z_2 et z_3, et la tangence a lieu aux milieux des trois côtés.*

Preuve.
On ne perd rien à supposer que P est unitaire, ainsi $P = (X - z_1)(X - z_2)(X - z_3)$ et $P' = 3(X - w_1)(X - w_2)$.

En vertu du théorème de Gauss-Lucas, les points w_1 et w_2 sont à l'intérieur du triangle de sommets z_1, z_2 et z_3.

Soit w_1' le symétrique de w_1 par rapport à la droite (z_1, z_2). On définit l'ellipse $\mathcal{E} = \{z \in \mathbb{C}, |z - w_1| + |z - w_2| = |w_1' - w_2|\}$.

Soit I l'intersection des droites (w_1', w_2) et (z_1, z_2). Alors $I \in \mathcal{E}$ car $|I - w_1| + |I - w_2| = |I - w_1'| + |I - w_2| = |w_1' - w_2|$. De plus, on voit par construction de w_1' que (z_1, z_2) est la bissectrice extérieure de l'angle $\widehat{w_1 I w_2}$, si bien que $\mathcal{E}$ et (z_1, z_2) sont tangentes en I.

Montrons maintenant que $\mathcal{E}$ est tangente à la droite (z_1, z_3). D'après le lemme de Poncelet, il suffit que les angles orientés $\widehat{z_2 z_1 w_2}$ et $\widehat{w_1 z_1 z_2}$ sont égaux. Remarquant que $P'(z_1) = (z_1 - z_2)(z_1 - z_3) = 3(z_1 - w_1)(z_1 - w_2)$, on écrit que $3\dfrac{w_2 - z_1}{z_2 - z_1} = \dfrac{z_3 - z_1}{w_1 - z_1}$, d'où l'égalité des angles en prenant les arguments.

Le même argument montre que $\mathcal{E}$ est tangente à la droite (z_2, z_3).

Il reste juste à montrer que les points de tangence sont les milieux des côtés du triangle. Soit z_{23} le milieu du segment $[z_2, z_3]$. Pour montrer que la tangence a lieu en z_{23}, il suffit de montrer que (z_2, z_3) est la bissectrice extérieure de l'angle $\widehat{w_1 z_{23} w_2}$ (car on sait déjà que (z_2, z_3) est tangente à l'ellipse). On écrit que $P'(z_{23}) = (z_{23} - z_2)(z_{23} - z_3) = 3(z_{23} - w_1)(z_{23} - w_2)$, d'où $\dfrac{z_3 - z_{23}}{w_1 - z_{23}} = 3\dfrac{w_2 - z_{23}}{z_2 - z_{23}}$, et on a l'égalité des angles voulue en prenant les arguments. Le même raisonnement s'applique aussi bien aux deux autres côtés. Ceci termine la preuve. □

Leçons possibles

118 Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.
136 Coniques. Applications.
139 Applications des nombres complexes à la géométrie.
144 Problèmes d'angles et de distances en dimension 2 ou 3.
140 Angles : Définitions et utilisation en géométrie.

Références

?

6 Prolongement des identités algébriques

THÉORÈME. *Soient $n \in \mathbb{N}^*$ et $P \in k[X_1, ..., X_n]$ où k est un corps. Si P s'annule sur $S_1 \times ... \times S_n$, où les S_i sont des parties infinies de k, alors P est le polynôme nul.*

Preuve.
On raisonne par récurrence sur $n \in \mathbb{N}^*$.

Pour $n = 1$, le résultat est connu : un polynôme à une indéterminée à coefficients dans un corps ayant une infinité de zéros est le polynôme nul.

Supposons le résultat acquis pour un certain $n \in \mathbb{N}^*$ et soit $P \in k[X_1, ...X_{n+1}]$ un polynôme s'annulant sur $S_1 \times ... \times S_{n+1}$, où chaque S_i est une partie infinie de k.

Fixons $(x_1, ..., x_n) \in S_1 \times ... \times S_n$. Le polynôme $P(x_1, ..., x_n, X_{n+1})$ est un polynôme à une indéterminée à coefficients dans k s'annulant sur l'ensemble infini S_{n+1}, c'est donc le polynôme nul. En écrivant $P = \sum_{j \geqslant 0} P_j X^j \in k[X_1, ..., X_n][X_{n+1}]$, on a donc $P_j(x_1, ..., x_n) = 0$ pour tout j.

En faisant varier $(x_1, ..., x_n)$ dans $S_1 \times ... \times S_n$ et en appliquant le même raisonnement, on voit que chaque polynôme $P_j \in k[X_1, ..., X_n]$ s'annule sur $S_1 \times ... \times S_n$. Par hypothèse de récurrence, on a $P_j = 0$ pour tout j, ce qui prouve que P est le polynôme nul.

□

Une conséquence immédiate de ce théorème est que l'on peut identifier polynômes et fonctions polynômiales de plusieurs variables dans le cas où k est un corps infini. Plus précisément, on a un morphisme injectif d'algèbres

$$\begin{array}{ccc} k[X_1, ..., X_n] & \to & k^{k^n} \\ P & \mapsto & (x_1, ..., x_n) \mapsto P(x_1, ..., x_n) \end{array}$$

Donnons une autre application directe, dont une conséquence est le théorème de l'élément primitif (cf. développement 15).

Proposition. *Soit k un corps infini et E un espace vectoriel sur k. Alors E n'est pas réunion finie de sous-espaces stricts.*

Preuve.
Il suffit de montrer que si H_1, ..., H_p sont des hyperplans de $E \simeq k^n$, alors $\bigcup_{i=1}^p H_i \neq E$.

Soit l_i la forme linéaire non nulle associée à H_i, c'est un élément non nul de $k[X_1, ..., X_n]$. Si $\bigcup_{i=1}^p H_i = E$, le polynôme $\prod_i l_i$ s'annule sur E, c'est donc le polynôme nul. Il s'ensuit

que l'une des formes linéaires l_i est nulle (par intégrité de $k[X_1, ..., X_n]$), contrairement à l'hypothèse.

□

On peut encore citer ces deux applications immédiates, dont je laisse la démonstration :

Proposition. *Soit $P \in k[X_1, ..., X_n]$ avec $k = \mathbb{R}$ ou $\mathbb{C}$. Si P s'annule sur un ouvert de k^n, il est le polynôme nul.*

Proposition. *Soit P un polynôme non nul de $k[X_1, ..., X_n]$ avec $k = \mathbb{R}$ ou $\mathbb{C}$. Alors l'ensemble $\{P \neq 0\} \subset k^n$ est un ouvert dense de k^n.*

Le corollaire suivant, bien qu'immédiat, est crucial (il exprime la densité des ouverts non vides pour la topologie de Zariski) :

Corollaire. *Soient k un corps infini et Q un polynôme non nul $\in k[X_1, ..., X_n]$. Si $P \in k[X_1, ..., X_n]$ s'annule sur la partie $\{Q \neq 0\}$ de k^n, alors il est le polynôme nul.*

Preuve.
On a $P(x)Q(x) = 0$ pour tout $x \in k^n$. D'après le théorème, PQ est le polynôme nul. $k[X_1, ..., X_n]$ étant un anneau intègre et Q n'étant pas le polynôme nul, on en déduit que $P = 0$.

□

Comme application de ce corollaire, on peut montrer le théorème de Cayley-Hamilton :

Théorème (Cayley-Hamilton). *Soit A un anneau commutatif unitaire et $M \in \mathcal{M}_n(A)$. Alors M est annulée par son polynôme caractéristique χ_M.*

Preuve.
On commence par le cas où A est un corps infini. L'idée est d'utiliser la « densité » des matrices diagonalisables. Chaque coefficient de la matrice $\chi_M(M)$ est une fonction polynômiale en les n^2 coefficients de M. En vertu du corollaire précédent, il suffit de montrer que celle-ci s'annule sur un ensemble $\{Q \neq 0\}$, où Q est un polynôme non nul en n^2 variables.

On choisit pour Q la fonction $M \mapsto \mathrm{Disc}(\chi_M)$, qui est bien polynômiale en les n^2 coefficients de M, et non nulle. Plus précisément, les points où Q ne s'annule pas sont exactement les matrices dont toutes les valeurs propres dans une clôture algébrique $\bar{A}$ de A sont distinctes. De telles matrices sont diagonalisables dans $\bar{A}$, et dans ce cas il est clair que $\chi_M(M) = 0$. Ceci prouve le théorème de Cayley-Hamilton dans le cas où A est un corps infini.

La preuve se généralise immédiatement à tout anneau commutatif unitaire. En effet, chaque coefficient de la matrice $\chi_M(M)$ s'exprime comme un polynôme à coefficients entiers en les coefficients de M. Ces polynômes sont nuls car la preuve a été faite sur $\mathbb{Q}$, le résultat reste donc vrai sur $\mathbb{Z}$ et par suite sur tout anneau commutatif unitaire.

□

Leçons possibles
117 Algèbre des polynômes à n indéterminées ($n \geqslant 2$). Polynômes symétriques. Applications.
123 Déterminant. Exemples et applications.
126 Endomorphismes diagonalisables.
129 Polynômes d'endomorphismes. Polynômes annulateurs. Applications.

Références
Un cours d'agrégation de David Bourqui.

7 Théorème de Gauss (polygones réguliers constructibles)

On admet le théorème de Wantzel, qui donne une condition nécessaire et suffisante pour qu'un point du plan complexe soit constructible à la règle et au compas (sous-entendu, étant donnés les deux points d'affixes respectives 0 et 1) :

Théorème (Wantzel). *Un point d'affixe z est constructible si et seulement si z est dans une extension L de $\mathbb{Q}$ telle qu'il existe une tour d'extensions $\mathbb{Q} = L_0 \subsetneq L_1 \subsetneq ... \subsetneq L_r = L$ avec $[L_i : L_{i-1}] = 2$ $\forall i$.*

On propose de démontrer le théorème suivant :

Théorème (Gauss). *« Le » polygone régulier à n côtés ($n \geqslant 3$) est constructible si et seulement si n est de la forme $2^s p_1 ... p_r$, où les p_i sont des nombres premiers de* Fermat *distincts.*

Pour simplifier, on suppose qu'il s'agit du polygone régulier à n côtés inscrit dans le cercle unité de $\mathbb{C}$, et dont un des sommets est 1 (sinon, il faut supposer que l'on connaît un des côtés).

Rappelons qu'un nombre premier de Fermat est un nombre premier de la forme $2^k + 1$. On montre que k est nécessairement lui-même une puissance de 2.

Preuve.
Commençons par remarquer qu'une condition nécessaire et suffisante pour que le polygone régulier à n sommets soit constructible est que le nombre $\omega_n = e^{2i\pi/n}$ soit constructible.

On commence par supposer que ω_n est constructible, il s'agit de montrer que n est de la forme annoncée.

On écrit *a priori* la décomposition de n en irréductibles : $n = 2^s {p_1}^{\alpha_1} ... {p_r}^{\alpha_r}$, où les p_i sont des nombres premiers $\geqslant 3$ deux à deux distincts et les α_i sont des entiers $\geqslant 1$.

Il est clair que si ω_n est constructible, alors ω_d est constructible si $d|n$ (par exemple, parce que $\omega_d = {\omega_n}^{n/d}$). On en déduit que les $\omega_{{p_i}^{\alpha_i}}$ sont constructibles. Or le polynôme minimal de $\omega_{{p_i}^{\alpha_i}}$ sur $\mathbb{Q}$ est $\phi_{{p_i}^{\alpha_i}}$ (car les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$), qui est de degré $\varphi({p_i}^{\alpha_i}) = {p_i}^{\alpha_i - 1}(p_i - 1)$. On a donc $[\mathbb{Q}(\omega_{{p_i}^{\alpha_i}}) : \mathbb{Q}] = {p_i}^{\alpha_i - 1}(p_i - 1)$, qui doit être une puissance de 2 d'après le théorème de Wantzel. On en déduit que p_i est un nombre de Fermat et $\alpha_i = 1$. n est donc de la forme annoncée.

Réciproquement, soit n un nombre entier $\geqslant 3$ de la forme $2^s p_1 ... p_r$, où les p_i sont des nombres premiers de Fermat distincts, et montrons que ω_n est constructible.

Commençons par remarquer que si deux nombres a et b sont premiers entre eux et tels que ω_a et ω_b sont constructibles, alors ω_{ab} est constructible. En effet, il existe alors deux entiers u et v tels que $au + bv = 1$ (théorème de BEZOUT), il suffit alors d'écrire que $\omega_{ab} = {\omega_a}^u {\omega_b}^v$. Par suite, il nous suffit de montrer que ω_{2^s} et les ω_{p_i} sont constructibles.

Il est clair que ω_{2^s} est constructible, d'après le théorème de WANTZEL : la tour $\mathbb{Q} \subset \mathbb{Q}[\omega_4] \subset ... \subset \mathbb{Q}[\omega_{2^s}]$ convient.

Il nous reste donc à montrer que $\omega = \omega_p$ est constructible si p est un nombre premier de FERMAT.

Le groupe $G = \mathcal{G}al(\mathbb{Q}[\omega]|\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^\times$ par $\sigma \mapsto m$ tel que $\sigma(\omega) = \omega^m$. Ainsi G est cyclique d'ordre $p - 1 = 2^q$.

Soit σ un générateur de G, et posons $L_k = \{z \in \mathbb{Q}(\omega), \sigma^{2^k}(z) = z\}$ pour $0 \leqslant k \leqslant q$. Les L_k sont des sous-corps de $\mathbb{Q}(\omega)$, et on a une tour d'extension $\mathbb{Q} = L_0 \subset ... \subset L_q = \mathbb{Q}(\omega)$.

De plus, $L_{k-1} \subsetneq L_k$. En effet, posons $x = \sum_{m=0}^{2^{q-k}-1} \sigma^{2^k m}(\omega)$. D'une part, il est clair que $x \in L_k$. D'autre part, $x \notin L_{k-1}$, car sinon on aurait $\sum_{m=0}^{2^{q-k}-1} \sigma^{2^{k-1}2m}(\omega) = \sum_{m=0}^{2^{q-k}-1} \sigma^{2^{k-1}(2m+1)}(\omega)$, ce qui est une égalité entre deux combinaisons linéaires différentes des éléments de la base $(1, \omega, ..., \omega^{p-1})$ de $\mathbb{Q}(\omega)$ sur $\mathbb{Q}$.

Ainsi, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^q = [L_q : L_{q-1}]...[L_1 : L_0]$ où $[L_k : L_{k-1}] > 1 \ \forall k$. On a donc nécessairement $[L_k : L_{k-1}] = 2 \ \forall k$. Ceci prouve que ω est constructible. □

Signalons que la dernière partie de la démonstration est réduite à presque rien dès lors qu'on connaît le théorème de correspondance de GALOIS.

Leçons possibles
(**109** Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.)
110 Nombres premiers. Applications.
(**112** Corps finis. Applications.)
(**113** Groupe des nombres complexes de module 1. Applications.)
(**116** Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.)
(**118** Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.)
(**120** Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications)
(**139** Applications des nombres complexes à la géométrie.)
140 Angles : Définitions et utilisation en géométrie.
(**141** Utilisation des groupes en géométrie.)

143 Constructions à la règle et au compas.
144 Problèmes d'angles et de distances en dimension 2 ou 3.

Références
[CL05]

8 Enveloppe convexe du groupe orthogonal

Soit $\mathcal{B}$ la boule unité fermée de $\mathcal{M}_n(\mathbb{R})$ pour la norme d'opérateur notée $\|.\|$ associée à la norme $\|.\|_2$ de $\mathbb{R}^n$.

THÉORÈME. *L'enveloppe convexe de $\mathcal{O}_n(\mathbb{R})$ est $\mathcal{B}$.*

Preuve.
Il est clair que $\mathcal{B}$ est convexe et $\mathcal{O}_n(\mathbb{R}) \subset \mathcal{B}$, si bien que $\mathrm{Conv}(\mathcal{O}_n(\mathbb{R})) \subset \mathcal{B}$.

On raisonne par l'absurde : supposons qu'il existe $A \in \mathcal{B}$, $A \notin \mathrm{Conv}(\mathcal{O}_n(\mathbb{R}))$.

Rappelons que $(X, Y) \mapsto \mathrm{tr}({}^tXY)$ est un produit scalaire sur $\mathcal{M}_n(\mathbb{R})$. En effet, cette application est bilinéaire symétrique, de plus si $X \in \mathcal{M}_n(\mathbb{R})$, ${}^tXX$ est une matrice symétrique positive. Ainsi, $\mathrm{tr}({}^tXX) \geqslant 0$ et $\mathrm{tr}({}^tXX) = 0 \Rightarrow {}^tXX = 0$, de sorte que $\|Xu\|^2 = 0\ \forall u \in \mathbb{R}^n$, finalement $X = 0$.

Soit P le projeté orthogonal de A sur le convexe compact $\mathrm{Conv}(\mathcal{O}_n(\mathbb{R}))$ relativement à ce produit scalaire. On sait que P est caractérisé par $\mathrm{tr}({}^t(A-P)(M-P)) \leqslant 0$ $\forall M \in \mathrm{Conv}(\mathcal{O}_n(\mathbb{R}))$, soit encore $\mathrm{tr}(BM) \leqslant \mathrm{tr}(BP)$ où on a noté $B = {}^tA - P$. On a aussi $\mathrm{tr}(BP) < \mathrm{tr}(BA)$, puisque $\mathrm{tr}(B(A-P)) = \mathrm{tr}({}^t(A-P)(A-P)) > 0$. Finalement, on peut écrire que $\mathrm{tr}(BM) < \mathrm{tr}(BA)\ \forall M \in \mathrm{Conv}(\mathcal{O}_n(\mathbb{R}))$.

Signalons que dans le paragraphe précédent, on a supposé connu le fait que l'enveloppe convexe d'un compact soit compacte, ce qui se déduit par exemple du théorème de CARATHÉODORY ; ainsi que le théorème de projection sur un convexe fermé dans un espace de HILBERT. On aurait pu aussi passer par le théorème de HAHN-Banach géométrique, mais ce n'est pas nécessaire ici.

Écrivons maintenant $B = \Omega S$ avec $\Omega \in \mathcal{O}_n(\mathbb{R})$ et $S \in \mathcal{S}_n^+(\mathbb{R})$ (décomposition polaire de B). D'après ce qui précède, on doit avoir $\mathrm{tr}(B\Omega^{-1}) < \mathrm{tr}(BA)$, soit $\mathrm{tr}S < \mathrm{tr}(\Omega SA)$. Soit $(e_1, ..., e_n)$ une base orthonormale de vecteurs propres de S. On a $\mathrm{tr}(\Omega SA) = \sum \langle \Omega SAe_i, e_i \rangle$, soit $\mathrm{tr}(\Omega SA) = \sum \langle Ae_i, S\Omega^{-1}e_i \rangle$. On en déduit que $\mathrm{tr}(\Omega SA) \leqslant \sum \|Ae_i\| \|S\Omega^{-1}e_i\|$, avec $\|Ae_i\| \leqslant 1$ (car $A \in \mathcal{B}$) et $\|S\Omega^{-1}e_i\| = \|Se_i\| = \lambda_i$, i-ème valeur propre de S. Ainsi, $\mathrm{tr}(\Omega SA) \leqslant \sum \lambda_i = \mathrm{tr}S$, contrairement à ce qui est écrit quelques lignes plus haut.

Pour conclure, on doit avoir $\mathrm{Conv}(\mathcal{O}_n(\mathbb{R})) \subset \mathcal{B}$, finalement $\mathrm{Conv}(\mathcal{O}_n(\mathbb{R})) = \mathcal{B}$.

□

Proposition. *$\mathcal{O}_n(\mathbb{R})$ est exactement l'ensemble des points extrémaux de $\mathcal{B}$.*

Preuve.
Soit $O \in \mathcal{O}_n(\mathbb{R})$, supposons que $O = \frac{1}{2}(U + V)$ avec U, $V \in \mathcal{B}$. Soit $x \in \mathbb{R}^2$, on a $\|Ox\|^2 = \|x\|^2$ d'une part et $\|\frac{1}{2}(Ux + Vx)\|^2 \leqslant 1$ d'autre part, en utilisant l'inégalité de

Cauchy-Schwarz et sachant que $\|Ux\|, \|Vx\| \leqslant 1$. Comme on est dans le cas d'égalité, on doit avoir $\|Ux\| = \|Vx\| = 1$ et Ux, Vx sont positivement liés. On en déduit que $Ux = Vx = Ox$, finalement $U = V = O$. Ceci montre que O est un point extrémal de $\mathcal{B}$.

Soit maintenant $M \in \mathcal{B} \setminus \mathcal{O}_n(\mathbb{R})$, on écrit $M = \Omega S$ avec $\Omega \in \mathcal{O}_n(\mathbb{R})$ et $S \in \mathcal{S}_n^+(\mathbb{R})$. On peut encore écrire $S = PDP^{-1}$, où D est diagonale et $P \in \mathcal{O}_n(\mathbb{R})$. Dire que $M = XDY \in \mathcal{B}$ avec X, $Y \in \mathcal{O}_n(\mathbb{R})$ et D diagonale revient à dire que les coefficients d_i de D sont dans $[-1, 1]$ (même si en l'occurrence ils sont $\geqslant 0$). Dire que $M \notin \mathcal{O}_n(\mathbb{R})$ revient à dire que l'un au moins des d_i est < 1. Pour $\alpha > 0$ assez petit, on a $[d_i - \alpha, d_i + \alpha] \subset [-1, 1]$. Si M_α désigne la matrice obtenue en remplaçant d_i par $d_i + \alpha$ dans D, alors M est le milieu du segment $[M_{-\alpha}, M_\alpha] \subset \mathcal{B}$, ce qui prouve que M n'est pas un point extrémal de $\mathcal{B}$. □

On remarquera que la première proposition se déduit immédiatement de la seconde si on connaît le théorème de Krein-Milman : un convexe compact est l'enveloppe convexe de ses points extrémaux.

Leçons possibles
106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.
132 Formes linéaires et hyperplans en dimension finie. Exemples et applications.
((**133** Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie.))
137 Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.
(**148** Groupe orthogonal d'une forme quadratique.)

Références

9 Automorphismes de $k(X)$

THÉORÈME. *Soit k un corps. Les automorphismes d'algèbre de $k(X)$ sont exactement les $F \mapsto F\left(\frac{aX+b}{cX+d}\right)$, où a, b, c, $d \in k$ et $ad-bc \neq 0$.*

Preuve.

Soit $\Phi : \mathrm{GL}_2(k) \to \mathrm{Gal}(k(X) : k)$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto F\left(\frac{aX+b}{cX+d}\right)$. On vérifie immédiatement que Φ est bien à valeurs dans l'ensemble des k-automorphismes de $k(X)$, qui est aussi l'ensemble des automorphismes d'algèbre de $k(X)$. De même, il est facile de voir que Φ est un morphisme de groupes. Le but est donc de montrer que Φ est surjectif.

Soit $\sigma \in \mathrm{Gal}(k(X) : k)$, notons $F \in k(X)$ l'image de X par σ. L'image de σ est $k(F)$, par surjectivité de σ on a $k(F) = k(X)$. En particulier $X \in k(F)$. Son polynôme minimal sur $k(F)$ est donc de degré 1. Par ailleurs, si on écrit $F = \frac{P}{Q}$ avec P et Q premiers entre eux alors le polynôme (en T et à coefficients dans $k(F)$) $\pi(T) = P(T) - FQ(T)$ annule X. Si on montre que π est irréductible sur $k(F)$, il sera donc de degré 1. Comme les coefficients dominants de $P(T)$ et $FQ(T)$ sont distincts (car F n'est pas dans k), on aura que P et Q sont des polynômes non proportionnels de degré 1, et le théorème sera montré.

Comme F est transcendant sur k, F peut être vu comme une indéterminée. Pour montrer que $P(T) - FQ(T)$ est un irréductible de $k(F)[T]$, il suffit de montrer que c'est un irréductible $k[F][T] \approx k[F,T] \approx k[T][F]$. Comme $P(T) - FQ(T)$ est un polynôme de $(k[T])[F]$ de degré 1 et de contenu 1, il est bien irréductible.

Au passage, on a immédiatement que $\mathrm{Ker}(\Phi) = k^* I_2$, si bien que $\mathrm{Gal}(k(X) : k) \approx \mathrm{PGL}_2(k)$. □

Leçons possibles

115 Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.

116 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Références

Francinou ?

10 Théorème de Frobenius-Zolotarev

Théorème (Frobenius-Zolotarev). *Soit p un nombre premier $\geqslant 3$ et V un espace vectoriel de dimension finie n sur $\mathbb{F}_p$. On note $\left(\frac{a}{p}\right)$ le symbole de* Legendre, *qui est égal à 1 si a est un carré dans $\mathbb{F}_p$ et -1 sinon.*
Soit $u \in GL(V)$. Si $\varepsilon(u)$ désigne la signature de u en tant qu'élément de $\mathfrak{S}_{p^n}$, alors $\varepsilon(u) = \left(\frac{det\ u}{p}\right)$.

Preuve.

$\mathrm{GL}(V)$ est un sous-groupe de $\mathfrak{S}_{p^n}$ donc la signature induit un morphisme de groupes encore noté $\varepsilon : \mathrm{GL}(V) \to \{\pm 1\}$ (par restriction). Le groupe $\{\pm 1\}$ étant commutatif, ε se factorise de manière unique selon le diagramme

$$\begin{array}{ccc} \mathrm{GL}(V) & \xrightarrow{\ \varepsilon\ } & \{\pm 1\} \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \bar{\varepsilon}} & \\ \mathrm{GL}(V)/D(\mathrm{GL}(V)) & & \end{array}$$

Or on rappelle que $D(\mathrm{GL}(V)) = \mathrm{SL}(V)$ (ici $p \geqslant 3$). En effet, il est clair d'une part que $D(\mathrm{GL}(V)) \subset \mathrm{SL}(V)$. Pour l'inclusion inverse, il suffit de montrer que toute transvection est un commutateur, $\mathrm{SL}(V)$ étant engendré par les transvections (ainsi que le montre l'algorithme du pivot de Gauss). Soit donc une transvection $u \in \mathrm{GL}(V)$. Comme $\mathrm{car}(\mathbb{F}_p) \neq 2$, u^2 est également une transvection. Or toutes les transvections du groupe linéaire d'un espace de dimension finie sont conjuguées : dans une base convenable, la matrice d'une transvection est $\begin{bmatrix} 1 & & \dots & 0 \\ & \ddots & & \vdots \\ \vdots & & 1 & 1 \\ 0 & \dots & & 1 \end{bmatrix}$ (c'est d'ailleurs leur forme réduite de Jordan). Il existe donc $v \in \mathrm{GL}(V)$ tel que $u^2 = vuv^{-1}$, soit encore $u = vuv^{-1}u^{-1}$: u est un commutateur.

Par ailleurs, le morphisme surjectif $\det : \mathrm{GL}(V) \to \mathbb{F}_p^*$ a pour noyau $\mathrm{SL}(V)$ (par définition), il se factorise donc de manière unique en un isomorphisme que nous noterons $\overline{\det} : \mathrm{GL}(V)/\mathrm{SL}(V) \to \mathbb{F}_p^*$ de sorte que l'on a le diagramme :

$$\begin{array}{ccccc} & & \mathrm{GL}(V) & \xrightarrow{\ \varepsilon\ } & \{\pm 1\} \\ & \swarrow{\scriptstyle \det} & \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \bar{\varepsilon}} & \\ \mathbb{F}_p^* & \xleftarrow[\overline{\det}]{} & \mathrm{GL}(V)/\mathrm{SL}(V) & & \end{array}$$

On obtient donc un morphisme $\delta : \mathbb{F}_p^* \to \{\pm 1\}$ tel que $\delta \circ \det = \varepsilon$. Le but est de montrer qu'il s'agit en fait du morphisme (symbole) de LEGENDRE.

Nous allons voir dans un premier temps que δ n'est pas le morphisme trivial ; il nous suffit d'exhiber $u \in \mathrm{GL}(V)$ tel que $\varepsilon(u) = \delta(\det u) = -1$. Pour cela on se souvient que V est isomorphe à $\mathbb{F}_q$ (en tant que $\mathbb{F}_p$-espace vectoriel), où $q = p^n$. Nous admettrons ici que le groupe multiplicatif d'un corps fini est cyclique, soit donc ω un générateur de $\mathbb{F}_q^*$. La multiplication par ω dans $\mathbb{F}_q$ est $\mathbb{F}_p$-linéaire, c'est donc un élément u de $\mathrm{GL}(V)$. De plus u est égal en tant que permutation au cycle $(1, w, w^2, ..., w^{q-2})$ qui est de longueur paire $q-1$, d'où $\varepsilon(u) = -1$, ce qu'on voulait.

Pour conclure, on montre qu'il n'existe qu'un morphisme de groupes non trivial de $\mathbb{F}_p^*$ vers $\{\pm 1\}$. On sait que le symbole de LEGENDRE et δ sont de tels morphismes. Mais $\mathbb{F}_p^*$ étant cyclique, tout morphisme $\mathbb{F}_p^* \to \{\pm 1\}$ est défini de manière unique (et bien défini) par l'image d'un générateur. Il en y a donc exactement deux : le morphisme trivial et celui qui envoie un générateur donné sur -1. On en déduit que δ est bien le symbole de Legendre, d'où $\forall u \in \mathrm{GL}(V)\ \varepsilon(u) = \delta \circ \det(u) = \left(\frac{\det u}{p}\right)$, ce qui termine la démonstration. □

Leçons possibles
101 Groupe opérant sur un ensemble. Exemples et applications.
103 Exemples de sous-groupes distingués et de groupes quotients. Applications.
104 Groupes finis. Exemples et applications.
105 Groupe des permutations d'un ensemble fini. Applications.
106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.
108 Exemples de parties génératrices d'un groupe.
110 Nombres premiers. Applications.
112 Corps finis. Applications.

Références
[BMP05] pp. 251-252 Exercice 5.4.
[Per96] pp. 96 et suivantes sur les transvections.

11 Comptage de racines et formes quadratiques

Soit $P \in \mathbb{R}[X]$ un polynôme de degré n. On note α_1, ..., α_n ses racines complexes (comptées avec multiplicité). On note $s_i = \sum_{k=1}^{n} \alpha_k^i$ pour $0 \leqslant i \leqslant n-1$). Les s_i sont réels car ce sont des fonctions symétriques des racines. Ainsi on peut les calculer de manière explicite (en fonction des coefficients de P), par exemple avec les formules de Newton.

Théorème. *Soit q la forme quadratique sur $\mathbb{R}^n$ définie par $q(u) = \sum_{0 \leqslant i,j \leqslant n-1} s_{i+j} u_i u_j$ où $u = (u_0, ..., u_{n-1}) \in \mathbb{R}^n$. Soit (s,t) la signature de q. Le nombre de racines réelles distinctes de q est $s-t$, tandis que le nombre de racines complexes distinctes est $s+t$ (i.e. le rang de q).*

Preuve.
On écrit $q(u) = \sum_{i,j} \sum_{k=1}^{n} \alpha_k^{i+j} u_i u_j$ soit $q(u) = \sum_{k=1}^{n} \sum_{i,j} \alpha_k^{i+j} u_i u_j$, soit encore $q(u) = \sum_{k=1}^{n} l_k(u)^2$ où $l_k(u) = \sum_{i=0}^{n-1} {\alpha_k}^i u_i$. Quitte à réordonner, on peut supposer que α_1, ..., α_r sont les racines complexes distinctes de P, avec des multiplicités respectives m_1, ..., m_r, ainsi $q = \sum_{k=1}^{r} m_k l_k^2 = \sum_{k=1}^{r} (\sqrt{m_k} l_k)^2$.

On a donc obtenu une décomposition sur $\mathbb{C}$ de q en somme de carrés de formes linéaires, de plus ces formes linéaires sont linéairement indépendantes car le déterminant des vecteurs de leurs r premières coordonnées (dans la base canonique de $\mathbb{R}^{n*}$) est un facteur près le déterminant de Van der Monde associé aux scalaires distincts α_1, ..., α_r.

Ainsi le rang de q sur $\mathbb{C}$ est r, c'est donc aussi son rang sur $\mathbb{R}$ (le rang d'une matrice ne dépend pas du corps de base, car il correspond à l'annulation d'un déterminant extrait). On a déjà la deuxième affirmation du théorème.

Maintenant, si l_k correspond à un α_k non réel, alors $\bar{l_k}$ correspond à $\bar{\alpha_k}$ qui a la même multiplicité m_k que α_k. Si on note $v_k = \frac{l_k + \bar{l_k}}{2}$ et $w_k = \frac{l_k - \bar{l_k}}{2i}$, alors les coefficients de v_k et w_k sont réels, et $m_k({l_k}^2 + \bar{{l_k}^2}) = 2m_k({v_k}^2 - {w_k}^2)$.

Ainsi, si α_1, ..., α_p sont les racines réelles distinctes de q et α_{p+1}, $\bar{\alpha_{p+1}}$, ..., α_{p+c}, $\bar{\alpha_{p+c}}$ ses racines complexes distinctes (avec $r = p+2c$), il vient $q = \sum_{k=1}^{p} m_k {l_k}^2 + \sum_{k=p+1}^{p+c} 2m_k({v_k}^2 - {w_k}^2)$. Ceci donne une décomposition de q sur $\mathbb{R}$ en somme de carrés de formes linéaires (réelles) qui sont linéairement indépendantes (on voit immédiatement que si elles étaient $\mathbb{R}$-liées, alors les l_k seraient $\mathbb{C}$-liées). La signature de q est donc $(p+c, c)$, d'où la première assertion du théorème.

□

Leçons possibles
118 Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.
131 Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.
(**132** Formes linéaires et hyperplans en dimension finie. Exemples et applications.)
145 Méthodes combinatoires, problèmes de dénombrement.

Références
gantmacher matrices t2 p199

12 Entiers de Gauss et théorème des deux carrés

On note $\mathbb{Z}[i]$ l'image de l'unique morphisme d'anneaux $\mathbb{Z}[X] \to \mathbb{C}$ qui envoie X sur i. On a immédiatement $\mathbb{Z}[i] \approx \mathbb{Z}[X]/(X^2+1)$ et $\mathbb{Z}[i] = \{a+ib, a, b \in \mathbb{Z}\}$. On l'appelle anneau des entiers de Gauss. Pour l'instant il s'agit au moins d'un anneau intègre.

Soit $N : \mathbb{Z}[i] \to \mathbb{N}$, $a+ib \mapsto a^2+b^2$.

Proposition.
– *N est multiplicative sur $\mathbb{Z}[i]$.*
– *Les inversibles de $\mathbb{Z}[i]$ sont $\{1, i, -1, -i\}$.*
– *$\mathbb{Z}[i]$ est euclidien pour le stathme N.*

Preuve.
Pour le premier point, il suffit d'écrire que $N(a+ib) = z\bar{z} = |z|^2$ où $z = a+ib$, il s'ensuit que $N(zz') = N(z)N(z')$.

Par conséquent, si z, $z' \in \mathbb{Z}[i]$ vérifient $zz' = 1$, on doit avoir $N(z)N(z') = 1$ donc $N(z) = N(z') = 1$. En écrivant $z = a+ib$, on a nécessairement $a = \pm 1$ et $b = 0$ ou l'inverse. Réciproquement, on vérifie immédiatement que ces nombres conviennent, finalement $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$.

Montrons maintenant le troisième point. Soient $z, z' \in \mathbb{Z}[i]$ avec $z' \neq 0$. Soit q un point de $\mathbb{Z}[i]$ le plus proche de $\frac{z}{z'}$ (au sens de la distance usuelle dans $\mathbb{C}$). Il est clair que q existe et $\left|\frac{z}{z'} - q\right| \leqslant \frac{\sqrt{2}}{2} < 1$ ($\frac{\sqrt{2}}{2}$ est le diamètre du domaine fondamental du réseau $\mathbb{Z}[i]$). Si on pose $r = z - z'q \in \mathbb{Z}[i]$, on a alors $z = z'q + r$ et $N(r) = |z - z'q|^2 = |z'|^2 \left|\frac{z}{z'} - q\right|^2$ d'où $N(r) < N(z')$ (y compris dans le cas où $r = 0$, mais peu importe).

□

Théorème. *Soit $p \in \mathbb{N}^*$ un nombre premier. Alors p est somme de deux carrés si et seulement si $p = 2$ ou $p = 1$ [4].*

Preuve.
Notons $\Sigma = \{a^2+b^2,\ a, b \in \mathbb{N}\}$. Il est facile de voir que les nombres de Σ sont égaux à 0, 1 ou 2 modulo 4. En particulier, la condition ci-dessus est nécessaire. Montrons maintenant qu'elle est suffisante.

Premièrement, on remarque qu'un nombre premier p est dans Σ si et seulement si p est réductible dans $\mathbb{Z}[i]$. En effet, si $p = a^2+b^2$, alors $p = (a+ib)(a-ib)$ et a et b sont non nuls donc $a+ib$ et $a-ib$ sont non inversibles, p est donc réductible dans $\mathbb{Z}[i]$. Réciproquement,

si $p = zz'$ avec $z,\ z' \in \mathbb{Z}[i]^\times$, alors $p^2 = N(z)N(z')$ avec $N(z),\ N(z') \neq 1$, si bien que $N(z) = N(z') = p$. p est donc somme de deux carrés.

$Z[i]$ est un anneau euclidien et en particulier factoriel, les irréductibles de $\mathbb{Z}[i]$ sont donc ses éléments premiers. Dire que p est un élément premier de $\mathbb{Z}[i]$ revient à dire (par définition) que l'anneau $\mathbb{Z}[i]/(p)$ est intègre. On a par des identifications classiques $\mathbb{Z}[i]/(p) \approx \mathbb{F}_p[X]/(X^2+1)$. Il s'ensuit que p n'est pas premier dans $\mathbb{Z}[i]$ si et seulement si -1 est un carré dans $\mathbb{F}_p$. On sait que cela équivaut à $p = 2$ ou $p = 3$ [4].

□

THÉORÈME. *Soit $n \in \mathbb{N}^*$, alors n est somme de deux carrés si et seulement si pour tout entier p premier (de $\mathbb{Z}$) tel que $p = 3$ [4], $\nu_p(n)$ est pair.*

Preuve.
Il est clair que la condition est suffisante car Σ est stable par multiplication. En effet, si $m = N(z)$ et $m' = N(z')$ alors $mm' = N(zz')$ est somme de deux carrés.

Réciproquement, supposons que $n \in \Sigma$ et soit p un entier premier égal à 3 modulo 4. D'après ce qu'on a vu dans la démonstration précédente, p est un élément premier de $\mathbb{Z}[i]$. Comme $n = a^2 + b^2$, on peut écrire $n = z\bar{z}$, avec $z = a + ib$. L'idéal engendré par p dans $\mathbb{Z}[i]$ étant stable par conjugaison, p divise z « autant de fois » que $\bar{z}$. Il s'ensuit que $\nu_p(n)$ est pair.

□

Leçons possibles
(**102** Sous-groupes discrets de R^n. Réseaux. Exemples.)
110 Nombres premiers. Applications.
111 Exemples d'applications des idéaux d'un anneau commutatif unitaire.
(**146** Anneaux principaux.)
114 Équations diophantiennes du premier degré $ax + by = c$. Autres exemples d'équations diophantiennes.

Références
[Sam03]

13 Théorème de Chevalley-Warning

On se place sur un corps fini $\mathbb{F}_q$ de caractéristique p.

Lemme. *Soit* $m \in \mathbb{N}$. $\displaystyle\sum_{x\in\mathbb{F}_q} x^m = \begin{cases} 0 & \text{si } m = 0 \text{ ou } q-1 \nmid m \\ -1 & \text{sinon} \end{cases}$

Preuve.
Si $m = 0$, $\sum_{x\in\mathbb{F}_q} x^m = \sum_{x\in\mathbb{F}_q} 1$ (sachant que $0^0 = 1$) soit $\sum_{x\in\mathbb{F}_q} x^m = q = 0$ dans $\mathbb{F}_q$.

Si $q-1 \nmid m$, soit g un générateur de ${\mathbb{F}_q}^\times$. $x \mapsto gx$ est une bijection de $\mathbb{F}_q$, on peut donc écrire $\sum_{x\in\mathbb{F}_q} x^m = \sum_{x\in\mathbb{F}_q} (gx)^m$ soit $\sum_{x\in\mathbb{F}_q} x^m = g^m \sum_{x\in\mathbb{F}_q} x^m$. Comme g est un générateur de ${\mathbb{F}_q}^\times$ et $q-1 \nmid m$, on a $g^m \neq 1$; on en déduit que $\sum_{x\in\mathbb{F}_q} x^m = 0$.

Enfin, si $m \neq 0$ et m est un multiple de $q-1$, alors $x^m = 1$ $\forall x \in {\mathbb{F}_q}^\times$. Il vient $\sum_{x\in\mathbb{F}_q} x^m = q-1 = -1$ dans $\mathbb{F}_q$.

□

Théorème (Chevalley-Warning). *Soit P_1, ..., P_r des polynômes non nuls de $\mathbb{F}_q[X_1, ..., X_n]$, tels que $\sum_{i=1}^r d^\circ P_i < n$. Alors $\#Z(P_1, ..., P_k) = 0$ [p].*

On a noté $Z(P_1, ..., P_k)$ l'ensemble des racines communes à tous les P_i dans ${\mathbb{F}_q}^n$.

Preuve.
Posons $S = \prod_{i=1}^r \left(1 - P_i^{q-1}\right)$. Montrons que S est la fonction caractéristique de $Z(P_1, ..., P_k)$ sur ${\mathbb{F}_q}^n$. Si $x \in {\mathbb{F}_q}^n$ est racine de tous les P_i, il est clair que $S(x) = 1$. Si $P_i(x) \neq 0$ pour un certain i, alors $P_i(x)^{q-1} = 1$ si bien que $S(x) = 0$. Ainsi, $\#Z(P_1, ..., P_k) = \sum_{x\in{\mathbb{F}_q}^n} S(x)$.

Écrivons $S(X) = \sum_\alpha \lambda_\alpha X^\alpha$ (où les α sont des multi-indices). On a alors $\sum_{x\in{\mathbb{F}_q}^n} S(x) = \sum_\alpha \lambda_\alpha \sum_{x\in{\mathbb{F}_q}^n} x^\alpha$. Fixons $\alpha = (\alpha_1, ..., \alpha_n)$, alors $\sum_{x\in{\mathbb{F}_q}^n} x^\alpha = \prod_{i=1}^n \sum_{x_i\in\mathbb{F}_q} {x_i}^{\alpha_i}$. Comme $\sum_{i=1}^r d^\circ P_i < n$, on a $d^\circ S = (q-1)\sum_{i=1}^r d^\circ P_i < n(q-1)$. Il s'ensuit que dans tout monôme de S, l'un au moins des α_i est $< q-1$. D'après le lemme précédent, on a alors $\sum_{x_i\in\mathbb{F}_q} {x_i}^{\alpha_i} = 0$. Finalement, on a $\sum_{x\in{\mathbb{F}_q}^n} S(x) = 0$ dans $\mathbb{F}_q$, ce qui prouve que $p \mid \sum_{x\in{\mathbb{F}_q}^n} S(x)$. □

Leçons possibles
(**109** Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.)
(**110** Nombres premiers. Applications.)

112 Corps finis. Applications.
117 Algèbre des polynômes à n indéterminées ($n \geqslant 2$). Polynômes symétriques. Applications.

Références
Cours d'arithmétique de Serre.

14 Matrices bistochastiques

Définition. *Une matrice $M \in M_n(\mathbb{R})$ est dite stochastique si elle est à coefficients positifs et si pour tout $1 \leqslant i \leqslant n$, on a $\sum_{j=1}^{n} m_{ij} = 1$.*

On dit que M est bistochastique (ou doublement stochastique) lorsque M et ${}^tM$ sont stochastiques.

Remarques.
- Une matrice M est stochastique si et seulement si $M \geqslant 0$ et $Mu = u$, où on a noté u le vecteur de $\mathbb{R}^n$ dont toutes les coordonnées sont 1.
- Si M est stochastique, alors $\|M\|_\infty = 1$ et $\rho(M) = 1$.
- L'ensemble des matrices stochastiques $\mathcal{S}$ est convexe et compact, ainsi que l'ensemble des matrices $\mathcal{B}$ des matrices bistochastiques.
- Les matrices de permutations sont bistochastiques.

Théorème (Birkhoff). *L'ensemble des matrices bistochastiques $\mathcal{B}$ est l'enveloppe convexe dans $M_n(\mathbb{R})$ de l'ensemble des matrices de permutations.*

Autrement dit, une matrice est bistochastique si et seulement si elle est barycentre de matrices de permutations.

Preuve.
Celle-ci repose sur le théorème de Krein-Milman, qui dit qu'un convexe compact d'un espace de dimension finie est l'enveloppe convexe de l'ensemble de ses points extrémaux.

$\mathcal{B}$ étant convexe et compact (dans $\mathrm{M}_n(\mathbb{R})$), il nous faut donc montrer que les matrices de permutations sont exactement les points extrémaux de $\mathcal{B}$. Rappelons qu'un point x d'un convexe $\mathcal{C}$ est extrémal s'il n'est à l'intérieur d'aucun segment de $\mathcal{C}$.

Il est clair que les matrices de permutations sont des points extrémaux de $\mathcal{B}$. Supposons en effet que l'on ait $P = \lambda M + (1-\lambda)N$, où P est une matrice de permutation, M, N sont éléments de $\mathcal{B}$ et $\lambda \in]0,1[$. Les matrices M et N étant à coefficients positifs, si $p_{ij} = 0$ on doit avoir $m_{ij} = n_{ij} = 0$. De même, les coefficients de M et N étant $\leqslant 1$, si $p_{ij} = 1$ on doit avoir $m_{ij} = n_{ij} = 1$. On en déduit que $M = N = P$, ce qui prouve que P est un point extrémal de $\mathcal{B}$.

Soit maintenant $M \in \mathcal{B}$ qui n'est pas une matrice de permutation. Il nous reste à montrer que M n'est pas un point extrémal de $\mathcal{B}$.

M n'étant pas une matrice de permutation, il existe un coefficient $m_{i_1 j_1} \in]0,1[$. Comme M est stochastique, il existe un indice j_2 tel que $m_{i_1 j_2} \in]0,1[$. De même, ${}^tM$ étant stochastique, il existe un indice i_2 tel que $m_{i_2 j_2} \in]0,1[$. On construit ainsi par récurrence une suite $(j_1, i_1, j_2, i_2, ...)$ telle que les coefficients $m_{i_k j_k}$ et $m_{i_k j_{k+1}}$ sont éléments de $]0,1[$. L'ensemble des indices étant fini, il arrive un moment où l'un des indices, de ligne ou de colonne, est répété.

On peut donc supposer que la suite $(i_1, j_1, i_2, ..., j_{r+1} = j_1)$ vérifie la propriété précédente, quitte à avoir commencé par le premier indice qui se répète. On construit alors une matrice B en posant $b_{i_k j_k} = 1$, $b_{i_k j_{k+1}} = -1$ (pour $1 \leqslant k \leqslant r$), $b_{ij} = 0$ sinon. Par construction, on a $Bu = 0$ et ${}^tBu = 0$. On en déduit que si $\alpha > 0$, les matrices $M + \alpha B$ et $M - \alpha B$ sont bistochastiques. De plus, on peut choisir α assez petit pour que ces matrices soient à coefficients $\geqslant 0$. Comme M est le milieu du segment $[M + \alpha B, M - \alpha B]$, il s'ensuit que M n'est pas un point extrémal de $\mathcal{B}$.

□

Corollaire. *Soit $\|.\|$ une norme sur $\mathbb{R}^n$ invariante par permutation des coordonnées. Alors $\|M\| = 1$ pour toute matrice bistochastique M.*

Preuve.
Par hypothèse, $\|P\| = 1$ pour toute matrice de permutation P. On en déduit que $\|M\| \leqslant 1$ pour toute matrice bistochastique M grâce au théorème précédent (par convexité de la norme subordonnée). Comme $Mu = u$, on a en fait $\|M\| = 1$. □

Leçons possibles
(**105** Groupe des permutations d'un ensemble fini. Applications.)
137 Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.

Références
[Ser01] pp. 59-60.

15 Théorème de l'élément primitif

Proposition. *Soit $K \to L$ une extension de degré fini. On note $[L : K]_s$ le nombre de K-morphismes de L dans $\bar{K}$, où $\bar{K}$ est une clôture algébrique de K.*
On a $1 \leqslant [L : K]_s \leqslant [L : K]$, et $[L : K]_s = [L : K]$ si et seulement si l'extension $K \to L$ est séparable.

On dira que $K \to L$ est séparable si tout élément de L est séparable sur K, *i.e.* annulé par un polynôme à coefficients dans K dont toutes les racines sont distinctes dans $\bar{K}$ (on dira aussi qu'un tel polynôme est séparable).

Preuve.
Puisque $K \to L$ est de degré fini, on peut écrire que $L = K[x_1, ..., x_n]$. On montre par récurrence que les extensions intermédiaires $L_k = K[x_1, ..., x_k]$ satisfont les propriétés annoncées.

Pour $k = 0$, c'est trivial, car $[K : K]_s = [K : K] = 1$ et l'extension $K \to K$ est séparable.

Supposons que les propriétés sont vérifiées pour L_k, montrons qu'elles le sont pour $L_{k+1} = L_k[x_{k+1}]$. En premier lieu, $[L_{k+1} : K]_s = [L_{k+1} : L_k]_s[L_k : K]_s$. En effet, tout K-morphisme $L_{k+1} \to \bar{K}$ est obtenu en prolongeant un K-morphisme $L_k \to \bar{K}$. Par hypothèse de récurrence, $[L_k : K]_s \leqslant [L_k : K]$. De plus, $[L_{k+1} : L_k]_s$ est le nombre de racine distinctes (dans $\bar{K}$) du polynôme minimal de x_{k+1} sur L_k, tandis que $[L_{k+1} : L_k]$ est son degré. On en déduit que $[L_{k+1} : L_k]_s \leqslant [L_{k+1} : L_k]$, ainsi on a bien $[L_{k+1} : K]_s \leqslant [L_{k+1} : L_k][L_k : K] = [L_{k+1} : K]$.

Vérifions maintenant la deuxième point. Si $K \to L_{k+1}$ est séparable, alors $K \to L_k$ est aussi séparable donc $[L_k : K]_s = [L_k : K]$ (par hypothèse de récurrence). De plus, x_{k+1} est séparable sur K donc sur L_k, par suite $[L_{k+1} : L_k]_s = [L_{k+1} : L_k]$. On a donc bien $[L_{k+1} : K]_s = [L_{k+1} : K]$. Maintenant si $K \to L_{k+1}$ n'est pas séparable, il existe un élément $x \in L_{k+1}$ qui n'est pas séparable. On a alors $[K(x) : K]_s < [K(x) : K]$, puis $[L_{k+1} : K]_s < [L_{k+1} : K]$.

□

Théorème. *Toute extension de degré fini séparable est monogène.*

Preuve.
Soit $K \to L$ une telle extension et notons $n = [L : K]_s = [L : K]$. On veut montrer qu'il existe un élément $x \in L$ de degré n sur K (on aura alors $L = K[x]$).

Par hypothèse, il existe des K-morphismes deux à deux distincts σ_1, ..., σ_n de L dans $\bar{K}$. On a donc $\mathrm{Ker}(\sigma_i - \sigma_j) \subsetneq L$ dès que $i \neq j$. Il s'ensuit que $\bigcup_{i<j} \mathrm{Ker}(\sigma_i - \sigma_j) \subsetneq L$, cf. la première proposition du développement 6. Montrons que $x \in L \setminus \bigcup_{i<j} \mathrm{Ker}(\sigma_i - \sigma_j)$ convient. Le polynôme minimal de x sur K admet tous les $\sigma_i(x)$ pour racines (dans $\bar{K}$), qui sont

deux à deux distincts. Ceci prouve que x est de degré $\geqslant n$ sur K, en fait de degré n (car $[K[x] : K] \leqslant [L : K] = n$). □

Leçons possibles
116 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
118 Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.
120 Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
(**132** Formes linéaires et hyperplans en dimension finie. Exemples et applications.)

Références
[Esc00]
[CL05]

16 Dénombrement des polynômes irréductibles sur un corps fini

La fonction de MÖBIUS $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ est définie par $\mu(n) = 0$ si n a un facteur carré, $\mu(n) = (-1)^s$ sinon, où s est le nombre de facteurs distincts dans la décomposition de n en irréductibles.

Lemme (Formule d'inversion de MÖBIUS)**.**
Soient f et g deux fonctions de $\mathbb{N}^*$ dans un groupe abélien G.
Si $\forall n\ f(n) = \sum_{d|n} g(d)$, alors $\forall n\ g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$.

Preuve.
Commençons par remarquer que μ est multiplicative au sens suivant : si n et m sont premiers entre eux, alors $\mu(nm) = \mu(n)\mu(m)$.

On introduit $S : \mathbb{N}^* \to G$, $n \mapsto \sum_{d|n} \mu(d)$. On a $S(1) = \mu(1) = 1$. Montrons que $S(n) = 0$ dès que $n > 1$. S est multiplicative au même titre que μ : si n et m sont premiers entre eux, alors $S(nm) = \sum_{d|nm} \mu(d) = \sum_{d|n, d'|m} \mu(dd')$ (car $d|nm \Leftrightarrow d = dd'$ avec $d|n$ et $d'|m$). De plus, deux nombres d et d' divisant respectivement n et m sont premiers entre eux (car n et m sont premiers entre eux), si bien que $S(nm) = \sum_{d|n, d'|m} \mu(d)\mu(d')$ soit encore $S(nm) = \left(\sum_{d|n} \mu(d)\right)\left(\sum_{d'|n} \mu(d')\right) = S(n)S(m)$. Il nous suffit donc de montrer que $S(p^\alpha) = 0$ dès que p est un nombre premier (et $\alpha \geqslant 1$). Il est clair que $S(p^\alpha) = \sum_{k=0}^{\alpha} \mu(p^k)$. Tous les termes de la somme sont nuls sauf le premier qui vaut 1 et le deuxième qui vaut -1. On a donc bien $S(p^\alpha) = 0$, par suite $S(n) = 0\ \forall n > 1$.

On peut maintenant montrer la formule d'inversion de MÖBIUS, partant du second membre B. Par une réindexation immédiate, on a $B = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$. En utilisant l'expression de f, il vient $B = \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} g(d')$. Or $\left(d|n \text{ et } d' \middle| \frac{n}{d}\right) \Leftrightarrow dd'|n \Leftrightarrow \left(d'|n \text{ et } d \middle| \frac{n}{d'}\right)$, on peut donc écrire $B = \sum_{d'|n} g(d') \sum_{d|\frac{n}{d'}} \mu(d)$ soit $B = \sum_{d'|n} g(d') S\left(\frac{n}{d'}\right)$. Comme $S\left(\frac{n}{d'}\right) = 0$ sauf si $d' = n$ (et dans ce cas $S\left(\frac{n}{d'}\right) = 1$), on trouve finalement $B = g(n)$, ce qu'il fallait.

□

THÉORÈME. *Soit $\mathcal{I}_{nq}$ l'ensemble des polynômes unitaires irréductibles de degré n sur le corps fini $\mathbb{F}_q$; notons I_{nq} son cardinal. On a* $I_{nq} = \dfrac{1}{n}\sum_{d|n} \mu\left(\dfrac{n}{d}\right) q^d$.

Preuve.
On commence par montrer que $X^{q^n} - X = \prod_{P\in\mathcal{I}_{dq} \text{ où } d|n} P$. Pour clarifier les choses, toutes les extensions algébriques de $\mathbb{F}_q$ seront vues comme des sous-corps d'une clôture algébrique fixée une fois pour toutes. Remarquons déjà que la décomposition en irréductibles de $X^{q^n} - X$ sur $\mathbb{F}_q$ est sans facteurs carrés car $X^{q^n} - X$ est scindé à racines simples dans $\mathbb{F}_{q^n}$.

Soit P un facteur irréductible (unitaire) de $X^{q^n} - X$, montrons que son degré d divise n. Soit α une racine de P, alors α est racine de $X^{q^n} - X$ donc $\alpha \in \mathbb{F}_{q^n}$. Il s'ensuit que $\mathbb{F}_q \subset \mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^n}$, d'où $[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)][\mathbb{F}_q(\alpha) : \mathbb{F}_q]$. P étant irréductible sur $\mathbb{F}_q$, P est le polynôme minimal de α sur $\mathbb{F}_q$ de sorte que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d$. D'autre part, $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. On a donc montré que d est un diviseur de n.

Réciproquement, soit $P \in \mathcal{I}_{dq}$ avec $d|n$, et montrons que $P|X^{q^n} - X$. Soit α une racine de P, alors P est le polynôme minimal de α sur $\mathbb{F}_q$, si bien que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d$. On en déduit que $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$ car $d|n$. Ainsi toute racine de P est racine de $X^{q^n} - X$, il s'ensuit que $P|X^{q^n} - X$ car P est séparable ($\mathbb{F}_q$ est un corps parfait).

En comparant les degrés, il vient $q^n = \sum_{d|n} dI_{dq}$. La formule d'inversion de MÖBIUS donne alors $nI_{nq} = \sum_{d|n} \mu\left(\dfrac{n}{d}\right) q^d$, d'où le résultat.

□

Leçons possibles
112 Corps finis. Applications.
116 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
(**118** Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.)
(**120** Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications)
145 Méthodes combinatoires, problèmes de dénombrement.

Références
mignotte algèbre concrète

17 Groupes finis de déplacements de l'espace

THÉORÈME. *Tout groupe fini de déplacements de l'espace s'identifie à un sous-groupe de SO(3) (et réciproquement) ; il est de l'un des cinq types suivants :*
- *Le groupe cyclique (isomorphe à $\mathbb{Z}/n\mathbb{Z}$) engendré par une rotation axiale d'angle $2\pi/n$ (où $n \in \mathbb{N}^*$) ;*
- *Le groupe diédral direct spatial d'un polygone régulier engendré par deux retournements d'axes concourant selon un angle de π/n (où $n > 1$), isomorphe à D_n ;*
- *Le groupe isomorphe à $\mathcal{A}_4$ des isométries d'un tétraèdre régulier ;*
- *Le groupe isomorphe à $\mathfrak{S}_4$ des rotations d'un cube ou d'un octaèdre régulier ;*
- *Le groupe isomorphe à $\mathcal{A}_5$ des rotations d'un dodécaèdre régulier ou d'un icosaèdre régulier.*

Preuve.
Soit G un tel groupe d'ordre $n \in \mathbb{N}^*$. L'orbite d'un point A est finie et son isobarycentre Ω est conservé par tous les éléments de G. Quitte à conjuguer G par la translation de vecteur $\overrightarrow{O\Omega}$, on peut donc supposer que $G \subset \mathrm{SO}(3)$.

Un élément non trivial $g \in G$ est donc une rotation dont l'axe coupe la sphère unité en deux points P et $-P$, appelés pôles de g. Soit $\mathcal{P}$ l'ensemble des pôles des éléments non triviaux de G. Le groupe G agit sur $\mathcal{P}$ par restriction. En effet, si P est un pôle de $g \in G \setminus \{\mathrm{id}_{\mathbb{R}^3}\}$, alors $h(P)$ est un pôle de la rotation $hgh^{-1} \in G$: il suffit d'écrire que $hgh^{-1}(h(P)) = hg(P) = h(P)$ puisque $g(P) = P$.

On note C_1, C_2, ..., C_k les orbites de $\mathcal{P}$ et p_i le cardinal du stabilisateur d'un élément de C_i, de sorte que $\#C_i = n/p_i$. A chaque couple $(P, -P)$ d'éléments de $\mathcal{P}$ tel que $P \in C_i$, on peut associer de manière unique $p_i - 1$ rotations non triviales de G. En comptant de la sorte les éléments de $G \setminus \{\mathrm{id}_{\mathbb{R}^3}\}$, on en déduit que $n - 1 = \dfrac{1}{2}\displaystyle\sum_{i=1}^{k}(p_i - 1)\#C_i$, soit encore $2 - \dfrac{2}{n} = \displaystyle\sum_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$. Comme $n \geqslant 2$, on a $1 \leqslant 2 - 2/n < 2$. D'autre part, on a $1/2 \leqslant 1 - 1/p_i < 1$ pour chaque i (car $p_i \geqslant 2$) ; on en déduit que l'on a nécessairement $k = 2$ ou 3.

Si $k = 2$, l'équation précédente s'écrit $2/n = 1/p_1 + 1/p_2$ soit encore $2 = \#C_1 + \#C_2$, on a nécessairement $\#C_1 = \#C_2 = 1$. Il y a donc seulement deux pôles opposés, on en déduit que G est le groupe cyclique engendré par une rotation d'axe passant par ces pôles et d'angle $2\pi/n$, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Si $k = 3$, on a nécessairement $n \geqslant 3$ et l'équation précédente se réécrit $1 + 2/n = 1/p_1 + 1/p_2 + 1/p_3$. On peut supposer $p_1 \geqslant p_2 \geqslant p_3$. Comme $1 + 2/n > 1$, on a nécessairement $p_3 = 2$. L'équation s'écrit alors $1/2 + 2/n = 1/p_1 + 1/p_2$. De nouveau, comme

$1/2 + 2/n > 1/2$, on doit avoir $p_2 = 2$ ou $p_2 = 3$. Examinons les différents cas :

- Si $p_2 = 2$, l'équation s'écrit $2/n = 1/p_1$, soit $n = 2p_1$. Par conséquent, n est pair et le stabilisateur G_1 des deux éléments $\{P_1, -P_1\}$ de C_1 est un sous-groupe de G d'indice 2, isomorphe à $\mathbb{Z}/(n/2)\mathbb{Z}$. Celui-ci agit transitivement sur les $n/2$ pôles de C_2 (ainsi que sur les $n/2$ pôles de C_3), tous contenus dans le plan médiateur de $\{P_1, -P_1\}$. Les éléments de C_2 sont les sommets d'un polygone régulier à $n/2$ côtés, dont le groupe des rotations s'identifie à G_1 et les symétries à la classe ne contenant pas $\{\mathrm{id}\}$ de G/G_1. Par conséquent, G est le groupe diédral spatial direct de ce polygone, isomorphe à D_n.

- Si $p_2 = 3$, l'équation s'écrit $1/p_1 = 1/6 + 2/n$. On en déduit que $3 \leqslant p_1 < 6$. On étudie ces trois sous-cas :
  - Si $p_1 = 3$, on a $n = 12$. G agit sur l'orbite C_1 qui a 4 éléments. Cette action est fidèle car seul $\mathrm{id}_{\mathbb{R}^3}$ stabilise > 2 points. G s'identifie donc à un sous-groupe d'indice 2 de $\mathfrak{S}_4$; finalement $G \approx \mathcal{A}_4$.

  - Si $p_1 = 4$, $n = 24$. L'orbite C_2 a 8 éléments. Tous les pôles d'ordre 3 (*i.e.* dont le stabilisateur est d'ordre 3) sont dans la même orbite. On en déduit que C_2 contient 4 pôles et leurs opposés (car un pôle et son opposé ont même ordre), notons-les P_1, $-P_1$, ..., P_4, $-P_4$. G agit sur ces couples de pôles (car une isométrie envoie deux point antipodaux sur deux points antipodaux). De plus, cette action est encore fidèle. En effet, si un élément non trivial $g \in G$ fixe les 4 couples de pôles, au moins trois couples sont « inversés », par exemple $\{P_1, -P_1\}$, $\{P_2, -P_2\}$, $\{P_3, -P_3\}$. Si P_1, P_2, P_3 forment une base de $\mathbb{R}^3$, on doit avoir $g = -\mathrm{id}_{\mathbb{R}^3}$: ce cas est exclu. Sinon, tous ces points sont dans un même plan. Mais un un élément du stabilisateur de P_1 d'ordre 3 envoie P_2 sur deux points n'appartenant pas au plan et non antipodaux, et seuls P_4 et $-P_4$ sont des points de C_2 qui ne sont (peut-être) pas dans notre plan : c'est absurde. Finalement, G s'identifie à un sous-groupe de $\mathfrak{S}_4$, pour des raisons de cardinal $G \approx \mathfrak{S}_4$.

  - Le cas $p_1 = 5$, $n = 60$ est admis. Une manière de le traiter serait de montrer que C_1 est un dodécaèdre régulier et que G s'identifie au groupe des rotations de ce dodécaèdre.

□

Leçons possibles
101 Groupe opérant sur un ensemble. Exemples et applications.
104 Groupes finis. Exemples et applications.
105 Groupe des permutations d'un ensemble fini. Applications.
107 Sous-groupes finis de $\mathrm{O}(2, \mathbb{R})$, de $\mathrm{O}(3, \mathbb{R})$. Applications.
133 Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie.

Références

[Lad03] pp377 et suivantes.

18 Théorèmes de Sylow

Théorème. *Soit G un groupe fini et p un nombre premier divisant $n = \#G$. On écrit $n = p^\alpha m$, où m est premier avec p.*

1. *G a au moins un p-Sylow. De plus, tout p-sous-groupe de G est contenu dans un p-Sylow.*

2. *Tous les p-Sylow sont conjugués (en particulier ils sont isomorphes).*

3. *Le nombre de p-Sylow divise m et il est congru à 1 modulo p.*

On peut rajouter que G a des sous-groupes d'ordre p^k pour tout $1 \leqslant k \leqslant \alpha$. C'est une conséquence immédiate du premier théorème de Sylow et de la proposition plus précise qui suit :

4. Si G est un p-groupe non trivial, il existe une suite de sous-groupes $\{e\} \subset G_1 \subset ... \subset G_{r-1} \subset G$ avec $G_i \triangleleft G_{i+1}$ et G_{i+1}/G_i cyclique d'ordre p (en particulier, un p-groupe est résoluble).

G a au moins un p-Sylow

Preuve.
On montre d'abord le lemme suivant : si H est un sous-groupe d'un groupe G et S un p-Sylow de G, alors il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.

H agit par translations à gauche sur l'ensemble G/S, on vérifie que le stabilisateur d'une orbite gS sous cette action est $H_{gS} = gSg^{-1} \cap H$. Supposons que ce sous-groupe de H ne soit jamais un p-Sylow de H. En vertu de l'égalité $H.gS = (H : H_{gS})$, p divise le cardinal de toutes les orbites. En sommant, on obtient que p divise le cardinal de G/S, ce qui est une contradiction.

Passons maintenant à l'existence d'un p-Sylow de G, avec les notations du théorème. On plonge G canoniquement dans $\mathfrak{S}_n$ puis dans $\mathrm{GL}_n(\mathbb{F}_p)$. En vertu du lemme, il nous suffit de montrer l'existence d'un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$. En comptant le nombre de bases de $\mathbb{F}_p^n$, on voit que $\#\mathrm{GL}_n(\mathbb{F}_p) = (p^n - 1)(p^n - p)...(p^n - p^{n-1})$ soit encore $\#\mathrm{GL}_n(\mathbb{F}_p) = p^{n(n-1)/2}m$ où $m = (p^n - 1)(p^{n-1} - 1)...(p - 1)$ est premier avec p. Soit $B \subset \mathrm{GL}_n(\mathbb{F}_p)$ l'ensemble des matrices de la forme $I_n + T$, où T est une matrice triangulaire supérieure stricte. Alors B est un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$ de cardinal $p^{n(n-1)/2}$, c'est donc un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.

□

Les points 1. 2. et 3.

Preuve.
Nous utiliserons le lemme suivant : Si H est un p-groupe agissant sur un ensemble X, alors

le nombre de points fixes de X sous l'action de H est égal à $\#X$ modulo p. C'est une conséquence directe de la formule des classes $\#X = \sum_i (H : H_{x_i})$.

Soient H un p-sous-groupe de G et S un p-Sylow de G. G agit sur l'ensemble de ses sous-groupes par conjugaison, notons X l'orbite de S. On a $\#X = (G : G_S)$, et comme G_S contient S, on en déduit que $\#X$ divise m (au fait, G_S est exactement le normalisateur de S dans G). H agit aussi sur X par restriction, comme p ne divise pas $\#X$ cette action a au moins un point fixe T (qui est un p-Sylow de G) d'après le lemme. On en déduit que H est contenu dans le normalisateur de T (par définition). Cela entraîne que $H \subset T$, admettons-le un instant, et le point **1.** est montré.

En prenant pour H un p-Sylow S' de G, on a nécessairement $S' = T$ (ils ont le même cardinal), si bien que S et S' sont conjugués et le point **2.** est montré. On voit en particulier que l'action de S' sur X a exactement un point fixe (à savoir S'), on a donc $\#X = 1 \mod p$ toujours grâce au lemme et aussi $\#X$ divise m (cf. plus haut), mais X est exactement l'ensemble des p-Sylow d'après **2.**, d'où le point **3.**

Enfin, reste à montrer ce que nous avions temporairement admis, à savoir que si un p-sous-groupe H est contenu dans le normalisateur $\mathrm{Nor}(S)$ d'un p-Sylow S, alors $H \subset S$. On voit facilement que HS est un sous-groupe de $\mathrm{Nor}(S)$ et que S est distingué dans HS. Ensuite, on remarque que l'application $h \mapsto h \mod S$ de H dans HS/S est surjective (en utilisant que $H \subset \mathrm{Nor}(S)$), et son noyau est exactement $H \cap S$. On en déduit que $(HS : S) = (H : H \cap S)$. Comme H est un p-groupe, si $H \cap S \neq H$, alors p divise $(H : H \cap S)$ donc $(HS : S)$, ce qui est exclu car S est un p-Sylow. On a donc $H \cap S = H$ *i.e.* $H \subset S$.

□

Le point 4.

Preuve.
Un p-groupe non trivial a un centre non trivial. En effet, G agit sur lui-même par conjugaison et la formule des classes donne $\#G = \#Z_G + \sum_i (G : G_{x_i})$, où la somme porte sur les orbites non réduites à un point. On en déduit que $0 = \#Z_G + 0 \mod p$, si bien que $\#Z_G$ n'est pas réduit à $\{e\}$.

Ensuite, on raisonne par récurrence sur α, où $\#G = p^\alpha$. Si $\alpha = 0$, il n'y a rien à faire. Si $\alpha \geqslant 1$, comme on sait que le centre de G est non trivial, on peut trouver un élément h d'ordre p dans le centre de G. Soit H le groupe cyclique engendré par h, H est d'ordre p et distingué dans G. G/H est donc un p-groupe d'ordre $p^{\alpha-1}$, et on peut appliquer l'hypothèse de récurrence : il existe $\{\overline{e}\}(= H) \subset \overline{G_1} \subset ... \subset \overline{G_{r-1}} \subset \overline{G}(= G/H)$ vérifiant les conditions voulues. On vérifie que la suite $\{e\} \subset H \subset G_1 \subset ... \subset G_{r-1} \subset G$ convient. □

Leçons possibles
101 Groupe opérant sur un ensemble. Exemples et applications.
103 Exemples de sous-groupes distingués et de groupes quotients. Applications.
104 Groupes finis. Exemples et applications.
105 Groupe des permutations d'un ensemble fini. Applications.

Références
[Lan04] pp35 et suivantes.
Un cours d'agrégation sur les-mathematiques.net.

19 Théorème de Burnside

Lemme. *Une matrice $N \in \mathcal{M}_n(\mathbb{C})$ est nilpotente si et seulement si $tr(N^k) = 0$ pour tout $1 \leqslant k \leqslant n$.*

Preuve.
Si N est nilpotente, toutes ses valeurs propres sont nulles ainsi que celles de ses itérées successives, d'où le résultat.

Réciproquement, si $\mathrm{tr}N^k = 0$ pour tout $1 \leqslant k \leqslant n$, les valeurs propres non nulles λ_1, ..., λ_r de N de multiplicités respectives α_1, ..., α_r vérifient $\alpha_1\lambda_1^k + ... + \alpha_r\lambda_r^k = 0$ pour tout $1 \leqslant k \leqslant r$. Si $r \geqslant 1$, le vecteur $(\alpha_1, ..., \alpha_r)$ est donc un zéro non trivial de la matrice $\Lambda = (\lambda_j^i)_{1\leqslant i,j\leqslant r}$ dont le déterminant se ramène immédiatement à un déterminant de Van der Monde par multilinéarité : $\det\Lambda = \lambda_1...\lambda_r \prod_{1\leqslant i<j\leqslant r}(\lambda_j - \lambda_i)$. Ce déterminant étant non nul, on aboutit à une contradiction. On doit donc en déduire que $r = 0$, autrement dit N est nilpotente.

□

Théorème (Burnside). *Un sous-groupe G de $GL_n(\mathbb{C})$ est d'exposant fini si et seulement si il est fini.*

Preuve.
Si G est fini, il est évidemment d'exposant fini (c'est une conséquence, par exemple, du théorème de Lagrange).

Réciproquement, supposons que G ait un exposant fini $e \in \mathbb{N}^*$. Soit $(C_1, ..., C_r)$ une famille d'éléments de G génératrice du sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ engendré par G (on pourra remarquer qu'il s'agit en fait d'une sous-algèbre). On définit $\tau : G \to \mathbb{C}^r$ par $\tau(A) = (\mathrm{tr}AC_1, ..., \mathrm{tr}AC_r)$. Nous allons montrer que l'application τ est injective : soient A, $B \in G$ telles que $\tau(A) = \tau(B)$.

On a alors $\mathrm{tr}AM = \mathrm{tr}BM$ pour tout $M \in G$ par linéarité de la trace, puisque les C_i engendrent un sous-espace contenant G. On en déduit que pour $k \in \mathbb{N}$, $\mathrm{tr}(AB^{-1})^{k+1} = \mathrm{tr}A[B^{-1}(AB^{-1})^k] = \mathrm{tr}B[B^{-1}(AB^{-1})^k]$ soit $\mathrm{tr}(AB^{-1})^{k+1} = \mathrm{tr}(AB^{-1})^k$, il s'ensuit par une récurrence immédiate que $\mathrm{tr}(AB^{-1})^k = \mathrm{tr}I_n = n$ pour tout $k \in \mathbb{N}$.

Notons $N = AB^{-1} - I_n$. N est diagonalisable car elle est annulée par le polynôme scindé à racines simples $(X + 1)^e - 1$ (puisque $(AB^{-1})^e = I_n$). De plus, on a pour $1 \leqslant k \leqslant n$ par la formule du binôme $N^k = \sum_{j=0}^k \begin{pmatrix} k \\ j \end{pmatrix} (AB^{-1})^j(-1)^{k-j}$, d'où on déduit que $\mathrm{tr}N^k = n\sum_{j=0}^k \begin{pmatrix} k \\ j \end{pmatrix} (-1)^{k-j} = n(1-1)^k$ soit $\mathrm{tr}N^k = 0$. D'après le lemme, il s'ensuit que N est nilpotente. Étant diagonalisable et nilpotente, N est la matrice nulle, ce qui revient à dire que $A = B$. Ceci prouve que τ est injective.

Les matrices de G étant annulées par le polynôme $X^e - 1$, leurs valeurs propres sont des racines e-èmes de l'unité. Les traces des éléments de G ne peuvent donc prendre qu'un nombre fini de valeurs. On en déduit que l'image de τ est finie, mais τ étant injective, cela entraîne que G est fini.

□

Leçons possibles
104 Groupes finis. Exemples et applications.
129 Polynômes d'endomorphismes. Polynômes annulateurs. Applications.
128 Endomorphismes nilpotents.
106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.

Références
[Ale99]

20 Théorème de Carlitz

Soit A un anneau commutatif unitaire. On appelle idéal fractionnaire de A tout sous-A-module I de $\mathrm{Frac}(A)$ tel qu'il existe $m \in A$, $mI \subset A$. L'ensemble des idéaux fractionnaires de A est muni d'une structure de monoïde commutatif pour la multiplication.

On dit que A est un anneau de Dedekind si ce monoïde est un groupe, autrement dit si pour tout idéal fractionnaire I il existe un idéal fractionnaire J tel que $IJ = A$. On peut signaler qu'une définition équivalente est de dire qu'un anneau de Dedekind est un anneau noethérien intégralement clos.

Comme exemples d'anneaux de Dedekind, on peut citer les anneaux principaux et les anneaux d'entiers des corps de nombres.

Nous admettrons une propriété essentielle des anneaux de Dedekind, à savoir que tout idéal fractionnaire non nul se décompose de manière unique en produit d'idéaux premiers et d'inverses d'idéaux premiers.

Lorsque A est anneau de Dedekind, on appelle groupe de Picard de A (ou groupe des classes d'idéaux de A) le quotient du groupe des idéaux fractionnaires par le sous-groupe des idéaux fractionnaires principaux. C'est un groupe abélien qu'on note $(\mathrm{Pic}(A), +)$.

Donnons une dernière définition : on dit qu'un anneau est semi-factoriel lorsque la longueur des factorisations en irréductibles d'un élément de l'anneau ne dépend que de cet élément. Autrement dit, si des irréductibles π_1, ..., π_r, τ_1, ..., τ_s vérifient $\pi_1 ... \pi_r = \tau_1 ... \tau_s$, alors $r = s$.

Théorème (Carlitz). *Soit A un anneau de* Dedekind *dont le groupe de* Picard *est fini. Alors A est semi-factoriel si et seulement si $\#Pic(A) \leqslant 2$.*

Preuve.
On commence par montrer deux lemmes.

Lemme 1. Soient $\mathfrak{p}_1$, ..., $\mathfrak{p}_r$ des idéaux premiers de A tels que $\mathfrak{p}_1 ... \mathfrak{p}_r = (\pi)$ avec $\pi \in A$ non inversible. Alors π est irréductible si et seulement si aucun sous-produit strict de $\mathfrak{p}_1 ... \mathfrak{p}_r$ n'est principal.

Supposons qu'il existe un sous-produit strict principal, par exemple $\mathfrak{p}_1 ... \mathfrak{p}_k = (\gamma)$. Notons $I = \mathfrak{p}_{k+1} ... \mathfrak{p}_r$. I est un idéal strict de A (car $I \subset (\pi)$). On a alors $\gamma I = (\pi)$. En particulier, il existe $\delta \in I$ tel que $\gamma\delta = \pi$. γ est non inversible car $(\gamma) \subset (\pi)$. δ est non inversible car sinon $(\gamma) = (\pi)$ et $I = A$, ce qui est exclu. Ceci montre que π n'est pas irréductible.

Réciproquement, supposons que π soit réductible, par exemple $\pi = \gamma\delta$ avec γ, δ non inversibles. Les idéaux γ et δ admettent des décompositions en produits d'idéaux premiers et d'inverses d'idéaux premiers. Par unicité de la décomposition de (π) en produit d'idéaux premiers (et d'inverses d'idéaux premiers), les précédents sont des sous-produits stricts de $\mathfrak{p}_1...\mathfrak{p}_r$.

Lemme 2. Soit $\mathfrak{p}$ un idéal premier de A dont la classe $\bar{\mathfrak{p}}$ est d'ordre r dans $\mathrm{Pic}(A)$. Alors $\mathfrak{p}^r = (\pi)$ avec π irréductible.

$\bar{\mathfrak{p}}^r = 0$ (dans $\mathrm{Pic}(A)$) donc $\mathfrak{p}^r$ est principal : $\mathfrak{p}^r = (\pi)$ avec π non inversible. D'après le lemme précédent, π est irréductible. En effet, s'il existait un sous-produit strict principal de $\mathfrak{p}^r$, alors $\bar{\mathfrak{p}}$ serait d'ordre $< r$.

Passons maintenant à la preuve du théorème.

Si $\#\mathrm{Pic}(A) = 1$, alors A est principal donc factoriel et *a fortiori* semi-factoriel.

Supposons maintenant que $\#\mathrm{Pic}(A) = 2$. Soit x un élément non nul et non inversible de A ayant une décomposition en produit d'éléments irréductibles $x = \pi_1...\pi_r\tau_1...\tau_s$, où on a noté π_i les facteurs premiers et τ_i ceux qui ne le sont pas. Il s'agit de montrer que l'entier $r + s$ est entièrement déterminé par x.
On écrit que $Ax = (A\pi_1)...(A\pi_r)(A\tau_1)...(A\tau_s)$. L'idéal $A\tau_i$ n'étant pas premier, il se décompose en produit d'idéaux premiers $\mathfrak{q}_{i1}...\mathfrak{q}_{it_i}$ avec $t_i \geqslant 2$. Le produit de deux idéaux non principaux étant principal (car $\#\mathrm{Pic}(A) = 2$), on a en fait $t_i = 2$ en vertu du premier lemme, par irréductibilité de τ_i. L'idéal Ax se décompose alors en produit d'idéaux premiers $(A\pi_1)...(A\pi_r)\mathfrak{q}_{i1}\mathfrak{q}_{i2}...\mathfrak{q}_{s1}\mathfrak{q}_{s2}$. Cette décomposition étant unique, le nombre de facteurs principaux l'est aussi ainsi que le nombre de facteurs non principaux, ce qui détermine r et s.

Enfin, supposons que $\#\mathrm{Pic}(A) \geqslant 3$, il s'agit d'exhiber des éléments de A qui contredisent sa semi-factorialité. On distingue deux cas :

– Il existe un élément g de $\#\mathrm{Pic}(A)$ d'ordre $m \geqslant 3$. La classe $-g$ est également d'ordre m. Soit $\mathfrak{p}$ et $\mathfrak{q}$ des représentants premiers de ces deux classes. Les idéaux $\mathfrak{p}^m$ et $\mathfrak{q}^m$ sont principaux, engendrés par des éléments irréductibles π et τ (d'après le second lemme). D'autre part, le produit $\mathfrak{pq}$ est principal et engendré par un élément irréductible θ d'après le premier lemme. On remarque que $(\mathfrak{pq})^m = \mathfrak{q}^m\mathfrak{q}^m$ soit encore $A\theta^m = A\pi\tau$, ce qui signifie qu'il existe u inversible tel que $\theta^m = u\pi\tau$. Comme $m \geqslant 3$, l'anneau A n'est pas semi-factoriel.

– S'il n'existe pas d'éléments d'ordre $\geqslant 3$ dans $\#\mathrm{Pic}(A)$, alors $\mathrm{Pic}(A) \approx (\mathbb{Z}/2\mathbb{Z})^d$ avec $d \geqslant 2$. On peut alors trouver des classes g et h telles que la classe $g + h$ soit non nulle et distincte de g et de h. Considérons alors des idéaux premiers $\mathfrak{p}$, $\mathfrak{q}$ et $\mathfrak{r}$ respectivement dans les classes g, h et $g + h$. Ces trois classes sont d'ordre 2 dans $\mathrm{Pic}(A)$ donc les idéaux $\mathfrak{p}^2$, $\mathfrak{q}^2$ et $\mathfrak{r}^2$ sont

principaux engendrés par des éléments irréductibles de A, notons-les $\mathfrak{p}^2 = A\pi$, $\mathfrak{q}^2 = A\tau$ et $\mathfrak{r}^2 = A\theta$. La classe $g+h+(g+h)$ est elle-même nulle donc l'idéal $\mathfrak{pqr}$ est principal engendré par un élément irréductible, notons-le $\mathfrak{pqr} = A\psi$. On remarque que $\mathfrak{p}^2\mathfrak{q}^2\mathfrak{r}^2 = (\mathfrak{pqr})^2$ donc $A\pi\tau\theta = A\psi^2$, ce qui montre que l'anneau A n'est pas semi-factoriel.

□

Leçons possibles
149 Groupes de petits cardinaux.
104 Groupes finis. Exemples et applications.
111 Exemples d'applications des idéaux d'un anneau commutatif unitaire.
108 Exemples de parties génératrices d'un groupe.

Références
?

21 Décomposition de DUNFORD effective

THÉORÈME. *Soit k un corps parfait et f un endomorphisme d'un k-espace vectoriel de dimension finie. Il existe alors d, $n \in k[f]$ tels que $f = d + n$, avec d semi-simple et n nilpotent. De plus, cette décomposition est effective lorsque k est de caractéristique* 0.

Il n'est pas dur de montrer qu'un tel couple est unique, en supposant simplement que $f = d + n$, avec d et n qui commutent, d semi-simple et n nilpotent. On insiste plutôt ici sur l'aspect effectif d'une telle décomposition, c'est-à-dire qu'il existe un algorithme permettant de la calculer (en un nombre fini d'étapes).

Preuve.
Soit P un polynôme non nul annulateur de f (par exemple son polynôme caractéristique). On écrit la décomposition de P en irréductibles : $P = {P_1}^{\alpha_1}...{P_r}^{\alpha_r}$. Notons $Q = P_1...P_r$. Q peut être calculé de manière effective si k est de caractéristique 0 car dans ce cas $P = \text{pgcd}(P, P')Q$. En effet, $P' = \sum_{i=1}^{r} \alpha_i {P_i}' {P_i}^{\alpha_i - 1} \prod_{j \neq i} {P_j}^{\alpha_j}$. Il est clair que $\forall i$ ${P_i}^{\alpha_i - 1}$ divise P', en revanche ${P_i}^{\alpha_i}$ ne divise pas P', car il divise tous les termes de la somme sauf le terme i (car on aurait alors $P_i | \alpha_i {P_i}'$, et $\alpha_i \neq 0$ dans k).

Soit $A = k[X]/(P)$, on note x la classe de X. Comme P annule f, on a un morphisme $\varphi : A \to k[f]$, $x \mapsto f$. Ainsi, si on trouve une décomposition $x = u + v$ avec $Q(u) = 0$ et v nilpotent dans A, alors $d = \varphi(u)$ et $n = \varphi(v)$ conviennent (d sera semi-simple car toujours annulé par Q, qui est sans facteurs carrés, et n sera toujours nilpotent). Notons que $P | Q^{\text{ppcm}(\alpha_i)}$, ainsi $Q(x)$ est nilpotent dans A.

Nous allons obtenir u grâce à la méthode de NEWTON : on construit la suite $(x_n)_{n \geqslant 0}$ telle que $x_0 = x$ et $x_{n+1} = x_n - \frac{Q(x_n)}{Q'(x_n)}$. Nous allons montrer par récurrence que $Q'(x_n)$ est inversible dans A (ainsi la suite est bien définie), et $Q(x_n) \in \left(Q(x)^{2^n}\right)$. Supposons un instant ceci démontré, alors la suite stationne (rapidement) car $Q(x)$ est nilpotent dans A. Soit u sa limite et posons $v = x - u$. Alors $Q(u) = 0$ et $v = \sum_{n \geqslant 0} x_{n+1} - x_n$ (la somme est finie) est nilpotent comme somme de nilpotents. Le théorème sera donc prouvé.

Initialisons la récurrence : d'une part il est clair que $Q(x_0) = Q(x) \in \left(Q(x)^{2^0}\right)$. D'autre part, Q' est premier avec P : on écrit $Q' = \sum_{i=1}^{r} {P_i}' \prod_{j \neq i} P_j$. $\forall i$, P_i ne divise pas Q' car il divise tous les termes de la somme sauf le terme i (sinon on aurait $P_i | {P_i}'$, ce qui est exclu car k est parfait). Il s'ensuit que $Q'(x)$ est inversible dans A (cela se voit en écrivant que $Q(X)U(X) + P(X)V(X) = 1$, ainsi $U(x)$ est l'inverse de $Q(x)$ dans A).

Vérifions maintenant l'hérédité de nos propriétés. Il est clair que $Q'(x_{n+1}) - Q'(x_n) \in (x_{n+1} - x_n)$. Or $(x_{n+1} - x_n) = (Q(x_n)) \subset \left(Q(x)^{2^n}\right)$, ainsi $Q'(x_{n+1})$ est inversible comme somme d'un inversible et d'un nilpotent. Enfin, la formule de TAYLOR donne $Q(x_{n+1}) = Q(x_n) - Q'(x_n)(x_{n+1} - x_n) + (x_{n+1} - x_n)^2 a$, où $a \in A$.

Sachant que $x_{n+1} - x_n = \frac{Q(x_n)}{Q'(x_n)}$, il vient $Q(x_{n+1}) = 0 + Q(x_n)^2 \frac{a}{Q'(x_n)}$, ce qui prouve que $Q(x_{n+1}) \in \left(Q(x_n)^2\right) \subset \left(Q(x)^{2^{n+1}}\right)$.

□

Leçons possibles

111 Exemples d'applications des idéaux d'un anneau commutatif unitaire.
(**146** Anneaux principaux.)
116 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
124 Réduction d'un endomorphisme en dimension finie. Applications.
(**125** Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.)
126 Endomorphismes diagonalisables.
128 Endomorphismes nilpotents.
129 Polynômes d'endomorphismes. Polynômes annulateurs. Applications.

Références

22 Action du groupe modulaire sur le demi-plan de Poincaré

On étudie le groupe modulaire $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I_2\}$ et son action sur le demi-plan de Poincaré $\mathbb{H} = \{z \in \mathbb{C}, \mathrm{Im}z > 0\}$.

L'opération par homographies

Rappelons que le groupe $\mathrm{PGL}_2(\mathbb{C}) = \mathrm{GL}_2(\mathbb{C})/\{-I_2, I_2\}$ agit fidèlement transitivement sur le la droite projective complexe $\mathrm{P}^1\mathbb{C}$, ses éléments sont appelés homographies.

On montre que l'opération de la classe d'une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$ prend l'expression suivante : $\overline{A} \star z = \dfrac{az+b}{cz+d}$, où la fonction $z \mapsto \frac{az+b}{cz+d}$ a été prolongée en une fonction continue $\mathrm{P}^1\mathbb{C} \to \mathrm{P}^1\mathbb{C}$.

$\mathrm{PSL}_2(\mathbb{Z})$ s'identifie à un sous-groupe de $\mathrm{PGL}_2(\mathbb{C})$ (grâce à l'isomorphisme $\mathrm{PGL}_2(\mathbb{C}) \approx \mathrm{PSL}_2(\mathbb{C})$), il agit donc sur $\mathrm{P}^1\mathbb{C}$ par restriction.

Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ et $z \in \mathbb{C}$, on a $\mathrm{Im}\overline{A} \star z = \mathrm{Im}\dfrac{(az+b)(c\overline{z}+d)}{|cz+d|^2} = \dfrac{ad-bc}{|cz+d|^2}\mathrm{Im}z$ soit $\mathrm{Im}\overline{A} \star z = \dfrac{\mathrm{Im}z}{|cz+d|^2}$. Ceci prouve que $\mathbb{H}$ est stable sous l'action de $\mathrm{PSL}_2(\mathbb{Z})$.

Enfin, l'action de $\mathrm{PSL}_2(\mathbb{Z})$ sur $\mathbb{H}$ reste fidèle : $\overline{A} \star z = z \Leftrightarrow cz^2 + (d-a)z - b = 0$, si cette égalité est vérifiée pour tout $z \in \mathbb{H}$ (qui est infini) cela impose $c = b = 0$ et $a = d$, et $\det A = 1$ entraîne $A = \pm I_2$ d'où $\overline{A} = \mathrm{id}$.

Un domaine fondamental de l'action

Notons $\mathcal{D} = \{z \in \mathbb{H}, |\mathrm{Re}z| \leqslant 1/2 \text{ et } |z| \geqslant 1\}$. Nous allons montrer que $\mathcal{D}$ est un domaine fondamental de l'action du groupe modulaire sur $\mathbb{H}$, c'est-à-dire que :
– toute orbite rencontre $\mathcal{D}$ en un ou deux points,
– si deux points de $\mathcal{D}$ sont dans une même orbite, alors ils sont sur la frontière de $\mathcal{D}$.

Nous allons voir que les matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ jouent un rôle particulier. Remarquons d'emblée que $\overline{T} \star z = z + 1$ et $\overline{S} \star z = -1/z$.

Fixons $z \in \mathbb{H}$. On cherche un point de partie imaginaire maximale dans l'orbite de z. Pour cela, on remarque que les parties imaginaires des points de $\mathcal{O}_z$ qui sont $\geqslant$ à celle de z forment un ensemble fini. En effet, $\mathrm{Im}\overline{A} \star z \geqslant \mathrm{Im}z \Leftrightarrow |cz + d| \leqslant 1$, et seul un nombre fini de couples $(c, d) \in \mathbb{Z}^2$ satisfont cette inégalité (pour le voir, on écrit que $|c|\mathrm{Im}z = |\mathrm{Im}(cz + d)| \leqslant 1$ impose que c soit borné, d'où on déduit sans mal que d est aussi borné). Comme $\mathrm{Im}\overline{A}\star z$ ne dépend que de c et d, notre affirmation s'en ensuit.

Soit donc $z_1 \in \mathcal{O}_z$ de partie imaginaire maximale. Quitte à translater z_1 grâce à T^n (où n est un élément de $\mathbb{Z}$ tel que $-1/2 \leqslant \mathrm{Re}z_1 + n \leqslant 1/2$), on peut supposer que $|\mathrm{Re}z_1| \leqslant 1/2$. De plus, on sait que $\mathrm{Im}\overline{S} \star z_1 \leqslant \mathrm{Im}z_1$ où $\mathrm{Im}\overline{S} \star z_1 = \dfrac{\mathrm{Im}z_1}{|z_1|^2}$, on en déduit que $|z_1| \geqslant 1$, et par suite $z_1 \in \mathcal{D}$. On a donc montré que chaque orbite rencontre $\mathcal{D}$.

Supposons maintenant que deux points z et z' de $\mathcal{D}$ soient dans une même orbite. On peut supposer que $\mathrm{Im}z' \geqslant \mathrm{Im}z$. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tel que $z' = \overline{A} \star z$. Conformément à ce qui a été écrit ci-dessus, on a alors $|c|\mathrm{Im}z \leqslant 1$ avec $\mathrm{Im}z > \sqrt{3}/2$ (car $z \in \mathcal{D}$), d'où on déduit que $|c| < 2$. Étudions les différents cas :

- Si $c = 0$, on a $\det A = ad = 1$, quitte à changer A en $-A$ on peut supposer $a = d = 1$. On a alors $z' = z + b$. Quitte à échanger les rôles de z et z' (ce qui n'a pas été fixé plus haut puisqu'ils ont même partie imaginaire), on peut supposer $b \geqslant 0$. Il est clair que l'on a alors nécessairement $b = 0$ (donc $A = I_2$) et $z' = z$ ou bien $b = 1$ et $\mathrm{Re}z = -1/2$. Dans ce dernier cas, z et z' sont sur la frontière de $\mathcal{D}$, de plus z' (ainsi que $\overline{A}$) est entièrement déterminé : il n'y a pas d'autres points de $\mathcal{D}$ dans l'orbite de z et z'.

- Si $c = 1$ (ce qui traite également le cas $c = -1$ quitte à changer A en $-A$), la condition $|z + d| \leqslant 1$ impose $d = 0$ et $|z| = 1$, $z = j$ et $d = -1$, ou $z = -1/j$ et $d = 1$ (faire un dessin). On distingue ces différents sous-cas :

  - Si $d = 0$, alors $b = -\det A = -1$ et $z' = a - 1/z$. $-1/z$ étant le symétrique de z par rapport à l'axe des imaginaires purs, cette situation n'est possible que si $a = 0$, ou $a = 1$ et $z = -1/j$, ou $a = -1$ et $z = j$. Ici aussi, dans chaque cas z et

z' sont sur la frontière de $\mathcal{D}$ et z' est entièrement déterminé par z : aucun autre point de l'orbite de z ne rencontre $\mathcal{D}$.

– Si $z = j$ et $d = 1$, on a alors $\det A = a - b = 1$, d'où on déduit que $z' = a + j$. Ceci n'est possible que si $a = 0$ ou $a = 1$. De nouveau, dans ces deux cas z et z' sont sur la frontière et aucun autre point de l'orbite de z ne rencontre $\mathcal{D}$.

– Si $z = -1/j$ et $d = -1$, la discussion est analogue.

Ceci termine la preuve que $\mathcal{D}$ est un domaine fondamental de l'action du groupe modulaire sur le demi-plan de POINCARÉ. On peut remarquer que pour obtenir une transversale « sympathique », il suffit d'enlever à $\mathcal{D}$ la droite $\mathrm{Re} z = 1/2$ et l'arc de cercle $\{e^{i\theta}, \pi/3 \leqslant \theta < \pi/2\}$.

S et T engendrent $\mathbf{SL}_2(\mathbb{Z})$

Quitte à modifier légèrement le début du paragraphe précédent en prenant z_1 de partie imaginaire maximale dans l'orbite de z sous l'action du sous-groupe G engendré par S et T, on voit que $\mathcal{D}$ contient au moins un point de chaque orbite de cette action (induite) de G sur $\mathbb{H}$.

Soit $A \in \mathrm{SL}_2(\mathbb{Z})$, on fixe $z \in \mathring{D}$ (par exemple $z = i$). Notons $z' = \overline{A} \star z$, il existe donc une matrice B de G telle que $\overline{B} \star z' \in \mathcal{D}$. Mais $\mathcal{D}$ étant un domaine fondamental de l'action du groupe modulaire sur $\mathbb{H}$, cela entraîne que $\overline{B} \star z' = z$, soit encore $\overline{BA} \star z = z$. L'étude menée au paragraphe précédent montre que l'on a de plus $BA = \pm I_2$, il s'ensuit que $A = \pm B^{-1}$. En remarquant que $S^2 = -I_2 \in G$, on en déduit que $A \in G$, si bien que $G = \mathrm{SL}_2(\mathbb{Z})$.

Leçons possibles
108 Exemples de parties génératrices d'un groupe.
103 Exemples de sous-groupes distingués et de groupes quotients. Applications.
102 Sous-groupes discrets de $\mathbb{R}^n$. Réseaux. Exemples.
101 Groupe opérant sur un ensemble. Exemples et applications.
138 Homographies de la droite complexe. Applications.
139 Applications des nombres complexes à la géométrie.
141 Utilisation des groupes en géométrie.

142 Exemples de propriétés projectives et d'utilisation d'éléments à l'infini.

Références
[Ale99] pp.81 et suivantes.

23 Groupes d'ordre 8

Proposition. *Les groupes d'ordre* 8*, à isomorphisme près, sont exactement* $(\mathbb{Z}/2\mathbb{Z})^3$*,* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$*,* $\mathbb{Z}/8\mathbb{Z}$*,* D_4 *et* $\mathbb{H}_8$*.*

Preuve.
Soit G un groupe d'ordre 8. Soit r le maximum des ordres des éléments de G.

Si $r = 8$, il existe un élément d'ordre 8 donc $G \approx \mathbb{Z}/8\mathbb{Z}$.

Si $r = 2$, alors G est abélien. En effet, soient x , $y \in G$, alors xy est d'ordre (au plus) 2. On en déduit que $xyxy = 1$, soit encore $xyx^{-1}y^{-1} = 1$ (tout élément de G est son propre inverse). Par suite, G est un espace vectoriel sur $\mathbb{F}_2$, de dimension 3 pour des raisons de cardinal. G est donc isomorphe à $\mathbb{F}_2^3$ en tant que $\mathbb{F}_2$-espace vectoriel et en particulier en tant que groupe.

Supposons maintenant que $r = 4$. Notons i un élément d'ordre 4 et $H = \langle i \rangle$. H est d'indice 2 dans G donc c'est un sous-groupe distingué. Rappelons rapidement pourquoi : soit $x \in G$ il s'agit de montrer que $xH = Hx$. Si $x \in H$, c'est évident. Sinon, on écrit la partition de G en classes à droite $G = H \sqcup xH$ (union disjointe) et en classes à gauche $G = H \sqcup Hx$, qui montre que $xH = Hx$.

On a donc une suite exacte $1 \to H \approx \mathbb{Z}/4\mathbb{Z} \to G \to G/H \approx \mathbb{Z}/2\mathbb{Z} \to 1$.

S'il existe un élément x d'ordre 2 dans G avec $x \notin H$, alors la flèche $G \to \mathbb{Z}/2\mathbb{Z}$ induit un isomorphisme du sous-groupe $\{1, x\}$ sur $\mathbb{Z}/2\mathbb{Z}$, si bien que la suite est scindée. G est donc isomorphe à un produit semi-direct $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

Sachant que $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \approx \mathbb{Z}/2\mathbb{Z}$, deux cas sont alors possibles : soit ρ est le morphisme trivial et le produit est direct (donc $G \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$) ; soit ρ est l'unique autre morphisme (l'identité modulo l'identification $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \approx \mathbb{Z}/2\mathbb{Z}$) et dans ce cas $G \approx D_4$.

Il reste donc le cas où $G \setminus H$ (G privé de H) ne contient que des éléments d'ordre 4. Soit $j \in G \setminus H$ et notons $k = ij$. On a $G = H \sqcup Hj = \{1, i, i^2, i^3, j, k, i^2j, i^2k\}$. On remarque que i^2 est le seul élément d'ordre 2 de G, en particulier $i^2 = j^2 = k^2$.

Montrons que le centre Z de G est le sous-groupe $\{1, i^2\}$. G n'est pas abélien car sinon i^2j^2 serait d'ordre 2, on aurait donc $i^2j^2 = i^2$ puis $j^2 = 1$ (ce qui est exclu puisque j est d'ordre 4). Z est donc au plus d'ordre 4. Mais si Z est d'ordre 4, alors G/Z est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (rappelons que Z est distingué dans G). G serait alors abélien : des éléments de la forme a^kz où $z \in Z$ commutent deux à deux. Z est donc d'ordre au plus deux. Enfin, montrons que $i^2 \in Z$: sachant que G est engendré par i et j, il suffit de montrer que $i^2j = ji^2$ (et $i^2i = ii^2$, mais c'est évident). Comme $i^2j \in G \setminus H$, il est d'ordre 4. Ainsi $(i^2j)^2$ est d'ordre 2, on a donc $i^2ji^2j = i^2$ d'où $ji^2j = 1$. Il s'ensuit que $i^2j = ji^2 = j^{-1}$. On a bien montré que $Z = \{1, i^2\}$, on notera désormais $i^2 = -1$.

Enfin, montrons que $-ji = k$. On sait déjà que $-ji \in G \setminus H$. $-ji = j$ et $-ji = -j$ sont exclus. De même, $-ji = -k$ est exclu car on aurait $ji = ij$, donc $j \in Z$. On a donc bien $-ji = k = ij$. Il s'ensuit facilement que $jk = -kj = i$ et $ki = -ik = j$. Ceci prouve que $G \approx \mathbb{H}_8$.

□

Leçons possibles
103 Exemples de sous-groupes distingués et de groupes quotients. Applications.
104 Groupes finis. Exemples et applications.
(**108** Exemples de parties génératrices d'un groupe.)
149 Groupes de petits cardinaux.

Références
Francinou et ses potes.

24 Pavage du plan

Un appelle groupe de pavage du plan euclidien $\mathbb{R}^2$ un groupe G de déplacements associé à un compact d'intérieur non vide P tel que :
(i) $G.P = \mathbb{R}^2$,
(ii) $\forall g, g' \in G$, $g.\mathring{P} \cap g'.\mathring{P} \neq \emptyset \Rightarrow g.P = g'.P$.

On appellera pavés tous les $Q = g.P$, où $g \in G$. La définition d'un groupe de pavage revient donc à dire que les pavés recouvrent le plan et sont d'intérieurs disjoints.

Notons τ_b la translation de vecteur $b \in \mathbb{C}$ et $r_{A;\theta}$ la rotation de centre A et d'angle θ.

THÉORÈME. *Il n'existe que cinq groupes de pavages du plan à conjugaison par une application affine près :*
– $\langle \tau_1, \tau_i \rangle$
– $\langle \tau_1, \tau_i, r_{O;\pi} \rangle$
– $\langle \tau_1, \tau_j, r_{O;2\pi/3} \rangle$
– $\langle \tau_1, \tau_i, r_{O;\pi/2} \rangle$
– $\langle \tau_1, \tau_{-j^2}, r_{O;\pi/3} \rangle$

En particulier, on voit que tout pavage du plan a un domaine fondamental P qui est en réalité convexe compact d'intérieur non vide.

Preuve.
Soit T l'ensemble des translations de G. T est un sous-groupe discret de $\mathbb{R}^2$. En effet, supposons qu'il existe des translations de vecteurs arbitrairement proches de 0 dans G. Soit $M \in \mathring{P}$, il existe alors une translation non nulle τ de G telle que $\tau(M) \in \mathring{P}$. D'après le premier point dans la définition d'un pavage, on a alors $\tau.P = P$, autrement dit P est stable par τ. Ceci est impossible car P est compact.

T est donc un sous-réseau dans $\mathbb{R}^2$: $T = \{0\}$ ou bien $T = \mathbb{Z}\vec{u}$ avec $\vec{u} \in \mathbb{R}^2 \setminus \{0\}$ ou bien $T = \mathbb{Z}\vec{u} \oplus \mathbb{Z}\vec{v}$ avec $\vec{u}$, $\vec{v} \in \mathbb{R}^2$ non colinéaires.

ON PEUT DIRE DÈS A PRÉSENT QUE LES ROTATIONS DE G STABILISENT T.

Si $T = \{0\}$, alors G est commutatif. En effet, si r, $s \in G$, alors $rsr^{-1}s^{-1}$ est une translation (sa partie linéaire est l'identité), donc $rsr^{-1}s^{-1} = \mathrm{id}_{\mathbb{R}^2}$. Les éléments de G sont donc des rotations de même centre Ω. Si $R > 0$ est assez grand pour que $P \subset D(\Omega, R)$, on a alors $G.P \subset D(\Omega, R)$, ce qui contredit la définition d'un pavage. Ce cas est donc exclu.

Supposons maintenant que $T = \mathbb{Z}\vec{u}$ avec $\vec{u} \in \mathbb{R}^2 \setminus \{0\}$. Si r est une rotation non triviale de G, alors $r\tau_{\vec{u}}r^{-1} = \tau_{\vec{r}(\vec{u})}$. On en déduit que $\vec{r}(\vec{u}) = -\vec{u}$. Les rotations non triviales de G sont donc toutes d'angle π. Maintenant si r, s sont des rotations non triviales de G, alors rs est une

translation de vecteur $2\overrightarrow{\Omega_s\Omega_r}$. On en déduit que tous les centres des rotations non triviales de G sont sur une droite Δ de direction $\mathbb{R}\vec{u}$. Par suite, si $R > 0$ est suffisamment grand pour que la bande $B = \{z \in \mathbb{C}, d(z, \Delta) < R\}$ contienne P, alors $G.P \subset B$, ce qui contredit encore la définition d'un pavage.

Finalement, $T = \mathbb{Z}\vec{u} \oplus \mathbb{Z}\vec{v}$ avec $\vec{u}$, $\vec{v} \in \mathbb{R}^2$ non colinéaires. Les éléments de $\vec{G}$ stabilisent ce réseau. En effet, si r est une rotation non triviale de G alors $r\tau_{\vec{b}}r^{-1} = \tau_{\vec{r}(\vec{b})}$, si bien que $\vec{r}(\vec{b}) \in T$. Dans la base $(\vec{u}, \vec{v})$, la matrice d'un élément r_θ de $\vec{G}$ est donc dans $\mathrm{GL}_2(\mathbb{Z})$. En particulier sa trace $2\cos\theta$ est un entier. On en déduit que $\theta \in \{0, \pi/3, \pi/2, 2\pi/3, \pi\}$.

En particulier $\vec{G}$ est fini donc cyclique. Soit $r \in G$ tel que $\vec{G} = \langle\vec{r}\rangle$. On a une suite exacte scindée $1 \to T \to G \to \vec{G} = \langle\vec{r}\rangle \to 1$. On peut donc écrire $G = T \ltimes \langle r\rangle$, en particulier G est engendré par $\tau_{\vec{u}}$, $\tau_{\vec{v}}$ et r.

Si $\theta = 0$ ou $\theta = \pi$, alors quitte à conjuguer par une transformation affine on peut supposer que O est le centre de r, $\vec{u} = 1$ ($\in \mathbb{C}$) et $\vec{v} = i$ (un tel changement de base envoie bien r sur $r_{O;\theta}$). Ceci donne les deux premiers cas du théorème.

Dans les autres cas, on écrit que l'on peut supposer $\vec{u} = 1$ et O centre de r quitte à conjuguer par une similitude. Si on pose $\vec{v}' = r(\vec{u})$, alors $(\vec{u}, \vec{v}')$ est une $\mathbb{Z}$-base de T (et alors $G = \langle\tau_{\vec{u}}, \tau_{\vec{v}'}, r\rangle$: on obtient bien les trois autres cas). En effet, sinon il existerait $n \in \mathbb{N}^*$ tel que $\vec{v}'/n \in T$ (par exemple grâce au théorème de la base adaptée), mais dans ce cas on devrait avoir $r^{-1}(\vec{v}'/n) = \vec{u}/n \in T$, ce qui n'est pas le cas.

Dessiner les pavages ne serait pas une mauvaise idée. □

Leçons possibles
101 Groupe opérant sur un ensemble. Exemples et applications.
102 Sous-groupes discrets de $\mathbb{R}^n$. Réseaux. Exemples.
(**103** Exemples de sous-groupes distingués et de groupes quotients. Applications.)
107 Sous-groupes finis de $O(2, \mathbb{R})$, de $O(3, \mathbb{R})$. Applications.
108 Exemples de parties génératrices d'un groupe.
((**133** Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie.))
135 Isométries d'un espace affine euclidien de dimension finie. Formes réduites. Applications.
(**139** Applications des nombres complexes à la géométrie.)
140 Angles : Définitions et utilisation en géométrie.
141 Utilisation des groupes en géométrie.
147 Applications affines.

(**144** Problèmes d'angles et de distances en dimension 2 ou 3.)

Références
goblot géométrie

25 Décomposition de Bruhat

Théorème. *Soit k un corps et $n \in \mathbb{N}^*$, alors $\mathrm{GL}_n(k) = \bigsqcup_{\sigma \in \mathfrak{S}_n} \mathcal{T} P_\sigma \mathcal{T}$, où $\mathcal{T}$ désigne le groupe des matrices triangulaires supérieures inversibles et P_σ la matrice de permutation associée à σ.*

Le fait que l'union soit disjointe donne en particulier l'unicité de la matrice de permutation associée à une matrice inversible donnée.

Preuve.
On commence par montrer l'existence de la décomposition. Soit $M = (m_{ij})_{1 \leqslant i,j \leqslant n} \in \mathrm{GL}_n(k)$. L'un au moins des coefficients de sa première colonne est non nul. Soit i_1 maximal tel que $m_{i_1 1} \neq 0$.

Pour $1 \leqslant i < i_1$, on effectue sur M l'opération élémentaire $L_i \leftarrow L_i - \frac{m_{i1}}{m_{i_1 1}} L_{i1}$. Cela revient à multiplier M à gauche par la matrice triangulaire supérieure inversible $T_{ii_1}\left(\frac{m_{i1}}{m_{i_1 1}}\right)$ (supérieure car $i_1 > i$). On a donc multiplié la matrice M par une matrice triangulaire supérieure inversible T_1 de sorte à obtenir une matrice M_1 dont tous les coefficients de la première ligne sont nuls sauf un. Quitte à multiplier (toujours à gauche) par une matrice de dilatation (triangulaire supérieure inversible), on peut supposer $m_{i1} = 1$.

On effectue ensuite les opérations élémentaires sur les colonnes $C_j \to C_j - m_{i_1 j} C_1$ pour $2 \leqslant j \leqslant n$. Cela revient à multiplier M à droite par des matrices triangulaires supérieures inversibles $T_{1j}(m_{i_1 j})$. À la fin de cette étape on a obtenu une matrice $M_1' = T_1 M T_1'$ de la forme suivante :

$$\begin{pmatrix} 0 & & & \\ \vdots & & * & \\ & & & \\ 0 & & & \\ 1 & 0 & \cdots\cdots & 0 \\ 0 & & & \\ \vdots & & * & \\ 0 & & & \end{pmatrix}$$

On recommence ensuite la même méthode à partir de la deuxième colonne, et ainsi de suite. On remarque que l'indice i_1 ne sera pas utilisé, ni l'indice i_2 après la deuxième étape, etc. À la fin de l'étape $n-1$ on obtient donc une matrice de permutation $P_\sigma = TMT'$ avec T, $T' \in \mathcal{T}$, d'où la décomposition voulue $M = T^{-1} P \sigma T'^{-1}$.

Démontrons maintenant l'unicité de P_σ dans une telle décomposition. Supposons que $T_1 P_\sigma T_2 = T_3 P_\tau T_4$ avec T_1, T_2, T_3, $T_4 \in \mathcal{T}$ et $\sigma \neq \tau$. On obtient donc des matrices T, $T' \in \mathcal{T}$ telles que $P_{\sigma^{-1}} T P_\tau = T'$. Soit i tel que $\sigma(i) < \tau(i)$. Il est clair qu'un tel i existe : considérer $\sum_{i=1}^n \sigma(i) = \sum_{i=1}^n \tau(i)$. Le coefficient non nul t_{ii} de T est « envoyé » en position $(\sigma(i), i)$ en multipliant T à gauche par $P_{\sigma^{-1}}$ puis en position $(\sigma(i), \tau(i))$ en multipliant à droite par τ. Comme $\sigma(i) < \tau(i)$, ce coefficient est dans la partie strictement inférieure de T', ce qui contredit le fait qu'elle soit triangulaire supérieure.

□

Donnons maintenant une application à l'action de $\mathrm{GL}_n(k)$ sur les drapeaux. On rappelle qu'un drapeau est une suite de sous-espaces vectoriels emboîtés $E_0 = \{0\} \subset E_1 \subset ... \subset E_n = k^n$ telle que $\dim E_k = k \ \forall k$. On note $\mathcal{D}$ l'ensemble des drapeaux.

Proposition. *Chaque orbite de $\mathcal{D} \times \mathcal{D}$ sous l'action de $GL_n(k)$ contient exactement un couple de la forme (I_n, P_σ) où P_σ est une matrice de permutation. En particulier, il y a $n!$ orbites.*

Preuve.
On commence par faire agir GL_n à gauche sur $\mathcal{D}$. Il est clair que cette action est transitive. On obtient donc une bijection entre le quotient de $\mathrm{GL}_n(\mathbb{R})$ par le stabilisateur du drapeau « canonique » (donné par $E_k = \langle e_1, ..., e_k \rangle$) et l'ensemble $\mathcal{D}$. Il est immédiat que ce stabilisateur est $\mathcal{T}$. De plus, l'action de $\mathrm{GL}_n(k)$ sur D s'identifie à celle de $\mathrm{GL}_n(k)$ sur $\mathrm{GL}_n(k)/\mathcal{T}$ (par multiplication).

Soit maintenant $(A, B) \in \mathcal{D} \times \mathcal{D} \approx \mathrm{GL}_n(k)/\mathcal{T} \times \mathrm{GL}_n(k)/\mathcal{T}$. Il est clair que $(A, B) \sim (I_n, A^{-1}B)$. On écrit alors la décomposition de Bruhat de $A^{-1}B$ soit $A^{-1}B = T P_\sigma T'$. On a donc $(A, B) \sim (I_n, T P_\sigma T') = (I_n, T P_\sigma)$ puis $(A, B) \sim (T^{-1}, P_\sigma) = (I_n, P_\sigma)$.

Reste à voir que deux tels éléments distincts ne sont pas dans la même orbite : si $(I_n, P_\sigma) \sim (I_n, P_\tau)$, il existe $M \in \mathrm{GL}_n(\mathbb{R})$ tel que $M = I_n$ et $M P_\sigma = P_\tau$ dans $\mathrm{GL}_n(k)/\mathcal{T}$. Il existe donc T, $T' \in \mathcal{T}$ telles que $M = T$ et $M P_\sigma = P_\tau T'$. On en déduit que $P_\sigma = T^{-1} P_\tau T'$, puis $\sigma = \tau$ d'après l'unicité dans la décomposition de Bruhat.

□

Leçons possibles
101 Groupe opérant sur un ensemble. Exemples et applications.
105 Groupe des permutations d'un ensemble fini. Applications.

122 Opérations élémentaires sur les lignes et les colonnes d'une matrice. Résolution d'un système d'équations linéaires. Exemples et applications.
130 Exemples de décompositions remarquables dans le groupe linéaire. Applications.

Références
Francinou algèbre 1

26 Décomposition polaire

THÉORÈME. *La multiplication $U(n) \times \mathcal{H}^{++} \to GL_n(\mathbb{C})$ est un homéomorphisme.*

Preuve.
Soit $M \in \mathrm{GL}_n(\mathbb{C})$, montrons qu'il existe un unique couple $(U, H) \in \mathrm{U}(n) \times \mathcal{H}^{++}$ tel que $M = UH$ (décomposition polaire).

Supposons que M se décompose de la sorte, alors on a $M^*M = H^2$. Comme $M^*M \in \mathcal{H}^{++}$, elle a une et une seule racine carrée dans $\mathcal{H}^{++}$, c'est ce qu'on montre ci-après. Une fois montrée l'unicité de H, celle de U s'en ensuit immédiatement (car $U = MH^{-1}$).

Montrons le point précédent : soient h' et h deux endomorphismes hermitiens définis positifs tels que $h^2 = h'$. $\mathbb{C}^n$ est somme directe des sous-espaces propres de h'. Soit E_λ un tel sous-espace, alors E_λ est stable par h (car h et h' commutent). h_F est encore hermitien défini positif donc diagonalisable, et toute valeur propre de h_F est une racine carrée d'une valeur propre de ${h'}_F$. Nécessairement, h_F n'a donc qu'une valeur propre, à savoir $\sqrt{\lambda}$: c'est une homothétie. h est donc uniquement déterminé sur les sous-espaces propres de h', donc sur $\mathbb{C}^n$. Réciproquement, on vérifie immédiatement que définir h de la sorte sur les sous-espaces propres de h' fournit bien une racine carrée hermitienne définie positive de h'.

Maintenant, si on prend pour H l'unique racine carrée dans $\mathcal{H}^{++}$ de M^*M et $U = MH^{-1}$, alors on a bien $M = UH$ et $U \in \mathrm{U}(n)$ car $U^*U = H^{-1}M^*MH^{-1} = I_n$ vu que $M^*M = H^2$.

Il est clair que l'application $(U, H) \mapsto UH$ est continue. Réciproquement, supposons que $M_k \overset{k\to+\infty}{\longrightarrow} M$ dans $\mathrm{GL}_n(\mathbb{C})$. Soit $M = U_kH_k$ (resp. $M = UH$) la décomposition polaire de M_k (resp. de M). Par compacité de $\mathrm{U}(n)$, on peut extraire une sous-suite convergente $\mathrm{U}_{\varphi(k)} \overset{k\to+\infty}{\longrightarrow} U'$ dans $\mathrm{U}(n)$. La suite de terme $H_{\varphi(k)} = {U_{\varphi(k)}}^* M_{\varphi(k)}$ converge alors vers $H' = {U'}^* M$. On voit que $H' \in \mathrm{GL}_n(\mathbb{C})$, de plus $H' \in \mathcal{H}^+$ (car $\mathcal{H}^+$ est fermé), finalement $H' \in \mathcal{H}^{++}$. Par unicité de la décomposition polaire, on a nécessairement $U' = U$ et $H' = H$. La suite (U_k) du compact $\mathrm{U}(n)$ n'a qu'une seule valeur d'adhérence, elle est donc convergente. On a ainsi $\mathrm{U}_k \overset{k\to+\infty}{\longrightarrow} U$ et $H_k = {U_k}^* M_k \overset{k\to+\infty}{\longrightarrow} U^*M = H$. Ceci prouve que m est bicontinue. □

Donnons maintenant une application :

Proposition. *$U(n)$ est un sous-groupe compact maximal de $GL_n(\mathbb{C})$.*

Preuve.
Soit G un sous-groupe compact de $\mathrm{GL}_n(\mathbb{C})$ contenant $\mathrm{U}(n)$. Soit $M \in G$ et $M = UH$ la décomposition polaire de M. Puisque $U \in G$, on a $H \in G$. La suite $(H^k)_{k\in\mathbb{N}}$ a donc une sous-suite convergente dans G (par compacité). Cela n'est possible que si toutes les valeurs propres de H (qui sont des réels > 0) sont $\leqslant 1$. Mais si l'une des valeurs propres de H est < 1, alors la limite d'une suite extraite de (H^k) est non inversible. Finalement, toutes les valeurs propres de H sont 1, donc $H = I_n$. Ainsi $M = U \in \mathrm{U}(n)$, ce qui montre que $G \subset \mathrm{U}(n)$.

□

Leçons possibles
106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications.
133 Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie.
134 Endomorphismes remarquables d'un espace vectoriel hermitien de dimension finie.
130 Exemples de décompositions remarquables dans le groupe linéaire. Applications.
(**203** Utilisation de la notion de compacité.)

Références
[Ser01]

27 Dénombrement des solutions d'une équation diophantienne

Soient α_1, ..., α_r des entiers non nuls premiers entre eux (dans leur ensemble). Pour chaque $n \in \mathbb{N}$, on considère l'équation diophantienne $(E_n) : \alpha_1 n_1 + ... + \alpha_r n_r = n$ (où l'inconnue est $(n_1, ..., n_r) \in \mathbb{N}^r$).

THÉORÈME. *L'équation diophantienne (E_n) a un nombre fini de solutions s_n que l'on peut calculer de manière explicite. De plus, $s_n \sim \dfrac{1}{\alpha_1 ... \alpha_r} \dfrac{n^r}{(r-1)!}$ quand $n \to +\infty$.*

Preuve.
Dans l'énoncé, le terme « explicite » signifie que nous allons donner une méthode pour calculer (en temps fini) une expression de s_n qui sera valable $\forall n$.

Soit $F(X) = \prod_{i=1}^{r} \dfrac{1}{1 - X^{\alpha_i}}$. D'une part, on a (dans $\mathbb{C}[[X]]$)

$$F(X) = \prod_{i=1}^{r} \sum_{n \geqslant 0} X^{n\alpha_i}$$

puis

$$F(X) = \sum_{n \geqslant 0} \sum_{n_1\alpha_1 + ... + n_r\alpha_r = n} X^n$$

d'où $F(X) = \sum s_n X^n$.

D'autre part, $F(X)$ admet une décomposition en éléments simples de la forme

$$F(X) = \sum_{\omega \in \bigcup \mu_{\alpha_i}(\mathbb{C})} \frac{a_{\omega,1}}{\omega - X} + ... + \frac{a_{\omega,m_\omega}}{(\omega - X)^{m_\omega}}$$

où on a noté $\mu_{\alpha_i}(\mathbb{C})$ le groupe des racines α_i-èmes de l'unité dans $\mathbb{C}$. Cette décomposition a lieu dans $\mathbb{C}(X)$ mais elle est valable dans $\mathbb{C}[[X]]$ car 0 n'est pas un pôle de F. On sait que les $a_{\omega i}$ peuvent être calculés de manière explicite.

Ensuite, on écrit que

$$\frac{1}{(\omega - X)^k} = \frac{1}{(k-1)!} \frac{\mathrm{d}^{k-1}}{\mathrm{d}X^{k-1}} \left(\frac{1}{\omega - X} \right)$$

d'où

$$\frac{1}{(\omega - X)^k} = \frac{1}{(k-1)!} \sum_{n \geqslant 0} (n+1)...(n+k-1)\omega^{-n-k} X^n$$

En reportant dans l'expression précédente de $F(X)$ et en identifiant les coefficients, on en déduit une expression de s_n.

Comme $F(X) = \prod_{i=1}^{r} \frac{1}{1-X^{\alpha_i}}$, 1 est un pôle de F d'ordre r. Tous les autres pôles ω sont d'ordre $m_\omega < r$. En effet, chaque polynôme $1 - X_i^{\alpha}$ est à racines simples, donc ω est un pôle d'ordre $\leqslant r$ de F et s'il était d'ordre r, il serait racine de chaque $1 - X^{\alpha_i}$. D'après l'identité de Bezout, il existe des entiers u_1, ..., u_r tels que $u_1\alpha_1 + ... + u_r\alpha_r = 1$ (car les α_i sont premiers entre eux). On obtiendrait alors $\omega = \omega^{u_1\alpha_1+...+u_r\alpha_r} = 1$.

Le terme général de la série $\frac{1}{(\omega - X)^k}$ est un $O(n^{k-1})$ (cf. ci-dessus, en se rappelant que $|\omega| = 1$), donc un $o(n^{r-1})$ sauf si $\omega = 1$ et $k = r$. On en déduit que dans l'expression de s_n, les contributions des $\frac{1}{(\omega - X)^k}$ sont négligeables devant celle de $\frac{1}{(1-X)^r}$. Ainsi, $s_n \sim a_{1,r}\frac{n^{r-1}}{(r-1)!}$ quand $n \to +\infty$.

Enfin, calculons $a_{1,r}$. Pour cela, on écrit que $a_{1,r} = (1-z)^r F(z)_{|z=1}$. Or $(1-X)^r F(X) = \prod_{i=1}^{r} \frac{1-X}{1-X^{\alpha_i}}$ soit encore $(1-X)^r F(X) = \prod_{i=1}^{r} \frac{1}{1+X+...+X^{\alpha_i-1}}$. Finalement, on a $a_{1,r} = \frac{1}{\alpha_1...\alpha_r}$, d'où le résultat attendu. □

Leçons possibles
114 Équations diophantiennes du premier degré $ax + by = c$. Autres exemples d'équations diophantiennes.
115 Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.
145 Méthodes combinatoires, problèmes de dénombrement.
224 Comportement asymptotique des suites numériques. Rapidité de convergence. Exemples.

Références
Gourdon, chambi ?

28 Théorèmes de Perron-Frobenius

Théorème (Perron-Frobenius, première forme faible). *Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice strictement positive (à coefficients > 0). Alors*
i) $\rho(A)$ est valeur propre et $\rho(A) > 0$.
ii) $\rho(A)$ est associé à un vecteur propre > 0.
iii) $\rho(A)$ est valeur propre simple, de plus c'est l'unique valeur propre de module maximal.

Preuve.
Soit $x \in \mathbb{C}^n$ tel que $Ax = \lambda x$ avec $|\lambda| = \rho(A)$. L'inégalité triangulaire donne $\rho(A)|x| = |Ax| \leqslant A|x|$. Supposons qu'on n'ait pas l'égalité, on a alors que $A|x| - \rho(A)|x| \geqslant 0$ est non nul. On en déduit que $A(A|x| - \rho(A)|x|) > 0$ (car $A > 0$), soit encore $\rho(A)v < Av$ avec $v = A|x| > 0$. Il existe alors un réel $\rho > \rho(A)$ tel que $\rho v \leqslant Av$. Par une récurrence immédiate, on a $\rho^k v \leqslant A^k v$ pour tout entier $k \geqslant 1$. Il s'ensuit que $\rho^k \|v\|_\infty \leqslant \|A^k\|_\infty \|v\|_\infty$ puis $\rho \leqslant \|A^k\|_\infty^{1/k}$. En passant à la limite quand $k \to \infty$ on obtient $\rho \leqslant \rho(A)$, ce qui est une contradiction.

On a montré que $A|x| = \rho(A)|x|$: $\rho(A)$ est valeur propre de A associé à $|x|$. Comme $|x| \geqslant 0$ est non nul et $A > 0$, on a $A|x| > 0$. Or $A|x| = \rho(A)|x|$ et $|x|$ a au moins une coordonnée non nulle, on en déduit que $\rho(A) > 0$ et le point i) du théorème est montré. Ensuite, toujours en vertu du fait que $A|x| = \rho(A)|x|$ avec $A|x| > 0$, et puisque $\rho(A) > 0$, on a nécessairement $|x| > 0$ et le point ii) est montré.

Ensuite, on remarque que l'on est dans le cas d'égalité de l'inégalité triangulaire $|Ax| \leqslant A|x|$, *i.e.* $\left|\sum_{j=1}^n a_{ij}x_j\right| = \sum_{i=1}^n a_{ij}|x_j|$ (sur chaque composante i). On en déduit que les x_j sont positivement liés (rappelons que $a_{ij} > 0$), autrement dit ils ont le même argument. On peut donc écrire $x = e^{i\theta}|x|$.

On en déduit d'une part que $\rho(A)$ est l'unique valeur propre de module maximal. En effet, en écrivant $Ax = \lambda x$ avec $|\lambda| = \rho(A)$, nous avons montré que $A|x| = \rho(A)|x|$ et $x = e^{i\theta}|x|$. On a donc $Ax = e^{i\theta}A|x| = e^{i\theta}\rho(A)|x|$ et par ailleurs $Ax = \lambda x = e^{i\theta}\lambda|x|$. En identifiant, il vient $\lambda = \rho(A)$, ce qu'on voulait.

D'autre part, on en déduit que $\rho(A)$ est valeur propre simple. Soit x et y deux vecteurs propres associés à $\rho(A)$, on veut montrer qu'ils sont colinéaires (sur $\mathbb{C}$). D'après ce qu'il précède ($|x|$, $|y|$ sont des vecteurs propres > 0 associés à $\rho(A)$, colinéaires à x et y respectivement), on peut supposer que $x > 0$ et $y > 0$. Soit $\beta = \min_{1 \leqslant i \leqslant n} \frac{y_i}{x_i}$. Par définition, on a $\beta x \leqslant y$ mais en fait forcément $\beta x = y$, car sinon en appliquant A il vient $\beta x < y$, ce qui contredit la définition de β. x et y sont donc colinéaires, et le point iii) est montré.

□

Théorème (Perron-Frobenius, seconde forme faible). *Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice positive (à coefficients positifs). Alors $\rho(A)$ est une valeur propre de A, associée à un vecteur propre positif.*

Première preuve.
Cette preuve repose sur la première forme faible.

Soit $A_k = A + \frac{1}{k}J$ (pour $k \in \mathbb{N}^*$), où J est la matrice dont tous les coefficients valent 1.

D'après la première forme faible du théorème de Perron-Frobenius, il existe un vecteur propre positif x_k, que l'on peut supposé normé, associé à la valeur propre $\rho(A_k)$. Quitte à extraire, on peut supposer que x_k a une limite x (qui est positif et normé) quand $k \to \infty$.

Nous aurons besoin du lemme suivant : si $0 \leqslant A \leqslant B$, alors $\rho(A) \leqslant \rho(B)$. En effet, on a dans ce cas $\|A^k\|_\infty \leqslant \|B^k\|_\infty$ pour tout entier k, et on a le résultat en passant à la limite quand $k \to \infty$.

Ici, on en déduit d'une part que $\rho(A) \leqslant \rho(A_k)$ pour tout k et d'autre part que $(\rho(A_k))_{k\in\mathbb{N}^*}$ est une suite décroissante. Elle converge donc vers $\rho \geqslant \rho(A)$.

En passant à la limite dans l'expression $A_k x_k = \rho(A_k)x_k$ quand $k \to +\infty$, il vient $Ax = \rho x$. Cela prouve que ρ est valeur propre de A associé au vecteur propre positif x, de plus on a $\rho \geqslant \rho(A)$ donc nécessairement $\rho = \rho(A)$, et le théorème est montré.

□

Deuxième preuve.
Cette preuve ne repose pas sur la première forme faible du théorème de Perron-Frobenius, mais elle utilise un corollaire du théorème du point fixe de Brouwer : toute application continue d'un convexe compact d'un espace de dimension finie dans lui-même admet un point fixe.

Soit $C = \{x \in \mathbb{R}^n, x \geqslant 0, \|x\|_\infty = 1 \text{ et } Ax \geqslant \rho(A)x\}$. On vérifie sans mal que C est convexe et compact. De plus C est non vide : soit $x \in \mathbb{R}^n$ normé tel que $Ax = \lambda x$ avec $\lambda = \rho(A)$, alors $\rho(A)|x| = |\lambda x| = |Ax| \leqslant A|x|$ donc $|x| \in C$.

S'il existe $x \in C$ tel que $Ax = 0$, on a nécessairement $\rho(A) = 0$ est le théorème est montré dans ce cas. Sinon, on définit la fonction f sur C par $f(x) = \frac{Ax}{\|Ax\|_\infty}$. On vérifie immédiatement que C est stable par f, il s'ensuit que f admet un point fixe $x \in C$. On a alors $Ax = \|Ax\|_\infty x$ si bien que x est un vecteur propre positif de A associé à la valeur propre $\|Ax\|_\infty$, de plus on doit avoir $\|Ax\|_\infty \geqslant \rho(A)$ d'où nécessairement $\|Ax\|_\infty = \rho(A)$.

□

Définition. *On dit qu'une matrice $A \in \mathcal{M}_n(k)$ (où k est un corps) est réductible s'il existe une partition non triviale $\{1, ..., n\} = I \cup J$ telle que $(i, j) \in I \times J$ entraîne $a_{ij} = 0$.*

Il est équivalent de dire qu'il existe une matrice de permutation P telle que $P^{-1}AP$ ait une forme triangulaire par blocs $\left[\begin{array}{c|c} * & * \\ \hline 0 & * \end{array}\right]$. On dit qu'une matrice est irréductible si elle n'est pas réductible.

Lemme. *$A \in \mathcal{M}_n(\mathbb{R})$ est irréductible si et seulement si $(I_n + |A|)^{n-1} > 0$.*

Preuve.
Si A est réductible, il existe une matrice de permutation P telle que $P^{-1}AP$ soit de la forme $\left[\begin{array}{c|c} * & * \\ \hline 0 & * \end{array}\right]$. On en déduit que $P^{-1}(I_n + |A|)^{n-1}P$ est également de la forme $\left[\begin{array}{c|c} * & * \\ \hline 0 & * \end{array}\right]$. Cette matrice contient des 0 donc $(I_n + |A|)^{n-1}$ aussi, P étant une matrice de permutation.

Pour la réciproque, on introduit la notion de chemin dans A : pour $1 \leqslant i, j \leqslant n$, on convient d'appeler chemin de i vers j dans A de longueur $m \in \mathbb{N}^*$ la donnée de $m-1$ indices $k_1, ..., k_{m-1}$ tels que a_{ik_1}, $a_{k_1k_2}$, ..., $a_{k_{m-1}j}$ soient tous non nuls. Par convention, il existe un unique chemin $i \to i$ de longueur 0.

Montrons par récurrence sur m qu'une condition nécessaire et suffisante pour qu'il existe un chemin de longueur m de $i \to j$ dans A est que $(|A|^m)_{ij} > 0$.

Les cas $m = 0$, $m = 1$ sont triviaux. Supposons le résultat vrai un certain $m \geqslant 1$. On a $(|A|^{m+1})_{ij} = \sum_{k=1}^{n} (|A|^m)_{ik}|a_{kj}|$. On en déduit que $(|A|^{m+1})_{ij} > 0$ si et seulement si il existe $k \in \{1, ..., n\}$ tel que $(|A|^m)_{ik} > 0$ et $|a_{kj}| > 0$. Par hypothèse de récurrence, cela revient à dire qu'il existe un chemin $i \to k$ de longueur m dans A et un chemin $k \to j$ de longueur 1. Il est clair que cela équivaut à l'existence d'un chemin $i \to j$ de longueur $m+1$ dans A.

On suppose que $((I + |A|)^{n-1})_{ij} = 0$. En écrivant que $((I + |A|)^{n-1})_{ij} = \sum_{k=0}^{n-1} \mathrm{C}_{n-1}^{k} (|A|^k)_{ij}$, on voit que cela équivaut à $(|A|^k)_{ij} = 0$ pour tout $0 \leqslant k \leqslant n-1$. Autrement dit, il n'existe pas de chemin $i \to j$ de longueur $\leqslant n-1$ dans A (en part. $i \neq j$). Comme on peut « extraire » de tout chemin $i \to j$ un chemin de longueur $\leqslant n-1$ (i et j étant distincts), on en déduit qu'il n'existe pas de chemin $i \to j$ dans A.

Soit $I = \{1 \leqslant k \leqslant n, \exists i \to k \text{ dans A}\}$ et $J = I^c$. Alors $I \neq \emptyset$ ($i \in I$) et $J \neq \emptyset$ ($j \in J$). De plus, si $(p, q) \in I \times J$, alors il n'existe pas de chemin $p \to q$ (sinon on construirait le chemin $i \to p \to q$). En particulier, $a_{pq} = 0$, ce qui prouve que A est réductible.

□

Théorème (Perron-Frobenius, forme forte). *Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice positive irréductible. Alors $\rho(A)$ est une valeur propre simple de A, associée à un vecteur propre strictement positif. De plus, $\rho(A) > 0$.*

Preuve.
D'après la deuxième forme faible du théorème de Perron-Frobenius, $\rho(A)$ est valeur propre de A, associée à un vecteur propre positif x. On écrit que $(I + A)^{n-1}x = (1 + \rho(A))^{n-1}x$. Or $(I + A)^{n-1} > 0$ (A étant irréductible) et $x \geqslant 0$ donc $(I + A)^{n-1}x > 0$. De plus il est clair que $(1 + \rho(A))^{n-1} > 0$, on en déduit que $x > 0$. Enfin, étant donné que $Ax = \rho(A)x$ avec Ax positif non nul et $x > 0$, on doit avoir $\rho(A) > 0$.

Il reste à montrer que $\rho(A)$ est valeur propre simple. Il nous suffit de montrer que c'est une racine simple du polynôme caractéristique χ_A, autrement dit que $\chi'_A(\rho(A)) \neq 0$.

En notant $V_1(X)$, ...,$V_n(X)$ les colonnes de la matrice $XI_n - A$, on a par multilinéarité du déterminant $\chi'_A(X) = \sum_{j=1}^n \det(V_1, ..., V_{j-1}, V'_j, V_{j+1}, ..., V_n)$. Étant donné que $V'_j = e_j$, le j-ème vecteur de la base canonique de $\mathbb{R}^n$, on peut écrire $\chi'_A(X) = \sum_{j=1}^n \det(V_1, ..., V_{j-1}, e_j, V_{j+1}, ..., V_n) = \sum_{j=1}^n \chi_{A_j}$, où A_j est la matrice obtenue en rayant les j-èmes lignes et colonnes dans A.

Soit B_j la matrice obtenue en annulant les j-èmes lignes et colonnes de A. Après une permutation, B_j est diagonale par blocs avec un bloc nul de taille 1 et le bloc A_j. On en déduit que $\rho(A_j) = \rho(B_j)$ et $0 \leqslant B_j \leqslant A$, mais $B \neq A$ puisque B est réductible. Il s'ensuit que $\rho(B_j) < \rho(A)$ (cf ci-dessous). Finalement, $\rho(A_j) < \rho(A)$ (pour tout j) donc $\chi_{A_j}(\rho(A)) > 0$ ($\rho(A)$ est strictement plus grand que la plus grande des racines réelles de χ_{A_j}, donc $\chi_{A_j}(\rho(A))$ est non nul et du signe de χ_{A_j} au voisinage de $+\infty$, c'est-à-dire > 0). On a donc $\chi'_A(X) > 0$.

Pour terminer la démonstration, il nous reste à montrer que si $0 \leqslant B \leqslant A$, avec A irréductible et $\rho(B) = \rho(A)$, alors $A = B$. Soit x un vecteur propre positif de B associé à $\rho(A)$ (seconde forme faible du théorème). On a $Ax \geqslant Bx = \rho(A)x$. Supposons que l'on ait pas $Ax = \rho(A)x$, alors en notant $v = (I + A)^{n-1}x$ il vient $Av - \rho(A)v = (I + A)^{n-1}(Ax - \rho(A)x) > 0$. Il existe donc $\rho > \rho(A)$ tel que $Av \geqslant \rho v$. On en déduit que pour tout entier k, $A^k v \geqslant \rho^k v$ puis $\|A^k\|_\infty \geqslant \rho^k$. En prenant la racine k-ème et en passant à la limite, on trouve $\rho(A) \geqslant \rho$: contradiction.

Remarque : Il n'est pas vrai que $\rho(A)$ est la seule valeur propre de plus grand module en général, en revanche on peut montrer que l'ensemble des valeurs propres de module maximal est de la forme $\rho(A)\mathbb{U}_p$, où $\mathbb{U}_p$ est le groupe des racines p-èmes de l'unité, et que le spectre de A est invariant par $\mathbb{U}_p$.

□

Leçons possibles
(**123** Déterminant. Exemples et applications.)
(**124** Réduction d'un endomorphisme en dimension finie. Applications.)
((**125** Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.))
(**129** Polynômes d'endomorphismes. Polynômes annulateurs. Applications.)
206 Utilisation de théorèmes de point fixe.

Références
[Via]
[Ser01]

Références

[Ale99] Michel Alessandri : *Thèmes de géométrie*. Dunod, 1999.

[BMP05] Vincent Beck, Jérôme Malick et Gabriel Peyré : *Objectif Agrégation (2e édition)*. H&K, 2005.

[CL05] Antoine Chambert-Loir : *Algèbre corporelle*. Éditions de l'École Polytechnique, 2005.

[Esc00] Jean-Pierre Escofier : *Théorie de Galois (2^e édition)*. Dunod, 2000.

[Lad03] Yves Ladegaillerie : *Géométrie affine, projective, euclidienne et anallagmatique*. ellipses, 2003.

[Lan04] Serge Lang : *Algèbre (3e édition)*. Dunod, 2004.

[Per96] Daniel Perrin : *Cours d'Algèbre*. ellipses, 1996.

[Pit06] Vincent Pit : Quelques développements d'agrégation. 2006.

[Sam03] Pierre Samuel : *Théorie algébrique des nombres (n-ième èdition)*. Hermann, 2003.

[Ser01] Denis Serre : *Les Matrices*. Dunod, 2001.

[Via] Grégory Vial : Cours de license d'algèbre linéaire numérique.