Liste des leçons d'algèbre

Gabriel Peyré

Le 5 octobre 2002

1 Liste des développements

1.1 Sous groupes compacts de GL(E)

Théorème 1.1. L'ÉNONCÉ À DÉMONTRER *E est un $\mathbb{R}$-ev de dimension n. Soit G un sous groupe compact de $GL(E)$. Alors il existe un produit scalaire $\langle .|. \rangle_G$ sur E, de forme quadratique q_G tel que $G \subset O(q_G)$.*

- *Si on suppose G fini, la réponse est évidente, il suffit de considérer* :

$$\forall (x,y) \in E^2, \langle x,y \rangle_G = \frac{1}{|G|} \sum_{g \in G} \langle g(x),g(y) \rangle$$

- *Construction d'un point fixe pour $v \in G$* : Si on suppose que l'on dispose d'un compact convexe non vide $K \subset E$ tel que pour un $v \in G$ fixé, on ait $v(K) \subset K$, on va construire un point fixe pour v. En effet, on prend $x_0 \in K$ et un considère la suite :

$$x_k = \frac{1}{k+1} \sum_{i=0}^{k} v^i(x_0)$$

- *Construction d'une norme strictement convexe stable par G* : On définit :

$$\forall x \in E, N^G(x) = \max_{g \in G} \|g(x)\| \tag{1}$$

- *Construction d'un point fixe pour G* : Cette fois ci, on suppose que l'on dispose d'un compact K stable par tous les éléments de G. Pour $u \in G$, on note $F_u = \{x \in E, u(x) = x\}$. Comme K est compact et les F_u fermé, Il suffit donc de montrer que pour toute famille finie $\{F_{u_k}\}_{k=1}^p$, on a $\bigcap_{k=1}^n F_{u_k} \neq \emptyset$. Pour ce faire, on construit $v = \frac{1}{p} \sum_{k=1}^p u_k$, qui vérifie $v(K) \subset K$. Reste à montrer que le point fixe a de v est un point fixe commun des u_k, ce qui provient de la stricte convexité de la norme N^G.
- *Une opération linéaire de G sur $\mathcal{S}_n$* : On note $\mathcal{S}_n$ l'espace vectoriel des matrices symétriques, et $\mathcal{S}_n^{++}$ le cône convexe des matrices symétriques définies positives. On note $*$ la loi symétrisée sur G, i.e. définie par $\forall (g_1,g_2) \in G^2, g_1 * g_2 = g_2 g_1$. On peut définir une action de $(G,*)$ sur $\mathcal{S}_n$ par via la formule $\forall g \in G, \forall S \in \mathcal{S}_n, gS = {}^t g S g$, ce qui correspond à la donnée du morphisme :

$$\begin{aligned} \rho :\ & (G,*) \to GL(\mathcal{S}_n) \\ & g \mapsto \rho(g) \quad \text{avec } \rho(g)(S) = {}^t g S g \end{aligned}$$

  On vérifie que ceci définit bien une action, ie $\rho(g_1 * g_2) = \rho(g_1)\rho(g_2)$ et $\rho(Id) = Id$. De plus, cette action est linéaire.

- *Construction de* $\langle .|. \rangle_G$: On note $\mathcal{G} = \rho(G) \subset GL(\mathcal{S}_n)$, qui est compact comme image continue de G compact par ρ continue (car polynomiale). Soit alors $\mathcal{S} = \{{}^t gg,\, g \in G\}$, compact comme image de G par $g \to {}^t gg$ continue car polynomiale, et est inclus dans $\mathcal{S}_n^{++}$, par construction (les éléments de G sont inversibles). On note K l'enveloppe convexe de $\mathcal{S}$, qui est à son tour compacte, d'après le théorème de *Carathéodory*, et incluse dans $\mathcal{S}_n^{++}$ qui est convexe. On remarque que, comme l'action de G est linéaire, comme $\mathcal{S}$ est stable par l'action de G, K l'est aussi, ce qui veut dire que K est stable par $\mathcal{G}$, qui est un sous groupe de $GL(\mathcal{S}_n)$. D'après l'étude menée aux paragraphes précédents, on peut donc trouver un élément $S \in K \subset \mathcal{S}_n^{++}$ fixe par tous les éléments de $\mathcal{G}$, ce qui signifie $\forall g \in G, \rho(g)(S) = {}^t gSg = S$ i.e. $G \subset O(q_S)$, où q_S est le produit scalaire euclidien défini par S.

Référence : [Ale99, p.141]
Utilisation : (***,4) (**,1) (*,0)
Mots clefs : compacité, point fixe, convexité, actions de groupe.

106	Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.	***
125	Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie.	***
129	Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.	***
144	Utilisation des groupes en géométrie.	***
101	Groupe opérant sur un ensemble. Exemples et applications.	**

1.2 Sous groupes compacts de GL(E), utilisation des ellipsoïdes de volume minimal

Référence : [Ale99, p.141]
Utilisation : (***,1) (**,1) (*,1)
Mots clefs : compacité, point fixe, convexité, extremum, déterminant, volume.

121	Déterminant. Applications.	***
106	Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.	**
129	Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.	*

1.3 Théorème de Brauer

Référence : [Fer01, p.0 (poly)]
Utilisation : (***,3) (**,5) (*,1)
Mots clefs : groupe de permutations, matrices semblables, actions de groupe.

105	Groupe des permutations d'un ensemble fini. Applications.	***
119	Matrices équivalentes. Matrices semblables. Applications.	***
141	Polynômes d'endomorphismes. Applications.	***
101	Groupe opérant sur un ensemble. Exemples et applications.	**
104	Groupes finis. Exemples et applications.	**
106	Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.	**
114	Groupe des nombres complexes de module 1. Applications.	**
121	Déterminant. Applications.	**
100	Méthodes combinatoires, problèmes de dénombrement. Séries génératrices.	*

1.4 Représentation linéaire des groupes finis

Définition 1.1. Représentation linéaire Soit V un $\mathbb{C}$-espace vectoriel de dimension finie n. Une *représentation linéaire* d'un groupe G dans V est la donnée d'un morphisme $\rho : G \to GL(V)$. Ceci correspond à la donnée d'une *action de groupe linéaire* de G sur V, en notant $\forall (g,v) \in G \times V$, $g.v = \rho(g)(v)$. On dit aussi que V est un G-module.

Exemple 1.2. Voici les exemples fondamentaux de représentations linéaires :

- La représentation triviale, définie par $\forall s \in G$, $\rho(s) = Id_V$.
- La représentation régulière : on se donne un espace vectoriel de dimension $|G|$ et on considère une base que l'on indice par les éléments de G, i.e. $\mathcal{B} = \{e_h\}_{h\in G}$. Pour $s \in G$, on définit alors $\rho(s) \in GL(V)$ par $\rho(s)(e_h) = e_{sh}$, ce qui correspond à une permutation des coordonnées.
- La représentation somme : pour deux représentations ρ^1 et ρ^2 respectivement sur V et W, on définit une représentation $\rho^1 \oplus \rho^2$ sur $V \oplus W$ par la formule :

$$\forall (v,w) \in V \times W,\ \rho^1 \oplus \rho^2(g)(v+w) = \rho^1(v) + \rho^2(w)$$

- La représentation produit : pour deux représentations ρ^1 et ρ^2 respectivement sur V et W, on définit une représentation $\rho^1 \otimes \rho^2$ notée aussi $\rho_{V\otimes W}$ sur $\mathcal{L}(V,W)$ (espace des applications linéaires de V dans W) par la formule :

$$\forall f \in \mathcal{L}(V,W),\ \rho_{V\otimes W}(g)(f) = \rho^2(g) \circ f \circ \rho^1(g^{-1})$$

- Une action sur les polynômes : si G est un sous-groupe fini de $GL_n(\mathbb{C})$, on définit une action linéaire de G sur $\mathbb{C}[X_1,\ldots,X_n]$ en notant, pour $A = (a_{i,j}) \in G$, $\rho(A)(P)$ le polynôme obtenu par la substitution de X_i par $\sum_{j=1}^n a_{i,j}X_j$. On note symboliquement $\rho(A)(P)(X) = P(A.X)$.

Définition 1.3. Représentations isomorphes Deux représentations ρ et ρ' d'un même groupe G respectivement sur V et V' sont dite *isomorphes* si il existe un isomorphisme $\tau : V \to V'$ tel que $\forall s \in G$, $\tau\rho(s) = \rho'(s)\tau$, ce qui permet d'identifier les deux représentations.

Définition 1.4. Sous représentations Si une représentation ρ de G sur V admet un sous espace vectoriel $W \subset V$ stable par tous les $\rho(s) \in GL(V)$, elle induit une sous représentation ρ^W sur W.

Définition 1.5. Représentations irréductibles Une représentation est dite *irréductible* si elle n'admet pas de sous représentation stricte.

Proposition 1.2. Représentation unitaire *Toute représentation est isomorphe à une représentation unitaire.*

Démonstration. On peut supposer V muni d'un produit hermitien $(.,.)$. Quitte à remplacer ce produit (x,y) par $\sum_{s\in G}(\rho(s)x,\rho(s)y)$, on peut supposer ce produit invariant par l'action de G. Donc dans une base orthonormale pour $(.,.)$, les matrices des $\rho(s)$ sont unitaires. □

Corollaire 1.3. *Une représentation ρ sur V est réductible si elle peut s'écrire comme somme $V = W \oplus W^0$ de deux représentations non triviales.*

Démonstration. Quitte à faire un changement de base, on peut supposer la représentation unitaire. Si la représentation n'est pas irréductible, elle admet un sous-espace globalement stable W, et en prenant un supplémentaire orthogonal W^0, ce dernier est aussi stable, car les matrices des $\rho(s)$ sont unitaires. □

Remarque. Le corollaire précédent signifie que les matrices des $\rho(s)$ sont diagonales par bloc dans une base bien choisie, ce qui correspond bien à la représentation somme.

Proposition 1.4. *Toute représentation peut s'écrire comme somme de représentations irréductibles.*

Remarque. Cette écriture n'est bien sûr pas unique, mais on va voir qu'elle est unique "à isomorphisme près", au sens que si $W = W_1 \oplus \ldots \oplus W_r$, le nombre de fois qu'une représentation irréductible U est isomorphe à un W_i est fixé.

Définition 1.6. Sous-représentation invariante Soit ρ une représentation sur V. On note V^G le sous-espace des vecteurs *invariants* , i.e. $V^G = \{v \in V;\ \forall s \in G,\ \rho(s)(v) := s.v = v\}$. C'est une sous représentation de V.

Définition 1.7. Opérateurs d'entrelacement Dans le cas de la représentation produit $\rho_{V\otimes W}$ sur $\mathcal{L}(V,W)$ de deux représentations ρ^1 et ρ^2 respectivement sur V et W, on note $Hom_G(V,W) := \mathcal{L}(V,W)^G$ l'espace des invariants. On nomme ses éléments des *opérateurs d'entrelacement* ou des *G-morphismes* .

Remarque. Dire que $f \in \mathcal{L}(V,W)$ est un opérateur d'entrelacement correspond à ce que f vérifie $\forall s \in G$, $f\rho^1(s) = \rho^2(s)f$, ie f fait commuter, pour tout $s \in G$, le diagramme :

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \downarrow{\scriptstyle \rho_V(s)} & & \downarrow{\scriptstyle \rho_W(s)} \\ V & \xrightarrow{f} & W \end{array}$$

Si f est bijectif, ceci correspond au fait que f soit un isomorphisme de représentations, dans le cas général, on parle de G-morphismes, où d'opérateurs d'entrelacement.

Lemme 1.5. Lemme de Schur *Soient $\rho^1 : G \to GL(V)$ et $\rho^2 : G \to GL(W)$ deux représentations irréductibles d'un groupe G. Soit $f \in \mathcal{L}(V,W)$ un opérateur d'entrelacement, ie $f \in Hom_G(V,W)$. Alors :*

- *Si ρ^1 et ρ^2 ne sont pas isomorphes, $f = 0$.*
- *Sinon, on peut supposer $V = W$, $\rho^1 = \rho^2$, et alors f est une homothétie.*

Démonstration. Si on suppose que $f \neq 0$, alors les hypothèses montrent que $V_0 = Ker(f)$ est stable par tous les $\rho^1(s)$, et donc comme ρ^1 est irréductible, $V_0 = \{0\}$. De même $Im(f)$ est stable par tous les $\rho^2(s)$, donc au final, f est un isomorphisme et ρ^1 et ρ^2 sont isomorphes.
Dans le deuxième cas, comme on travail sur des $\mathbb{C}$-espaces vectoriels, f a au moins une valeur propre λ. En posant $f' = f - \lambda Id$, on voit que $Ker(f') \neq \{0\}$, et en appliquant la première partie de la démonstration, on a $f' = 0$. □

Corollaire 1.6. *On a donc : $dim_{\mathbb{C}}(Hom_G(V,W)) = 1$.*

Définition 1.8. Opérateur de Reynolds Soit ρ une représentation de G sur V. On définit l'opérateur $R_G \in \mathcal{L}(V,V)$ par la formule :

$$R_G := \frac{1}{|G|}\sum_{s\in G}\rho(s) \qquad \in \mathcal{L}(V,V)$$

On l'appelle *opérateur de Reynolds* .

Théorème 1.7. Propriétés de l'opérateur de Reynolds *R_G est un projecteur sur V^G. En particulier :*

(i) $V^G = Im(R_G) = Ker(R_G - Id)$
(ii) $dim_{\mathbb{C}}(V^G) = tr(R_G)$

Définition 1.9. Application moyennée Dans le cas de la représentation produit $\rho_{V\otimes W}$ sur $\mathcal{L}(V,W)$ de deux représentations ρ^1 et ρ^2 respectivement sur V et W, pour $f \in \mathcal{L}(V,W)$, on node $\widehat{f} := R_G(f) \in \mathcal{L}(V,W)$, ce qui correspond à l'application moyennée :

$$\widehat{f} : v \in V \to \frac{1}{|G|}\sum_{s\in G}\rho^2(s)(f(\rho^1(s^{-1})(v)))$$

Proposition 1.8. Application aux G-morphismes *Dans le cas de la représentation produit $\rho_{V\otimes W}$ sur $\mathcal{L}(V,W)$ de deux représentations ρ^1 et ρ^2 respectivement sur V et W, pour $f \in \mathcal{L}(V,W)$, on a :*

$$dim_{\mathbb{C}}(Hom_G(V,W)) = tr(R_G) = \varepsilon$$

Avec $\varepsilon = +1$ si les deux représentations sont isomorphes, et 0 sinon. De plus, pour tout $f \in \mathcal{L}(V,W)$, $\widehat{f}$ est une application $G-$invariante pour la représentation linéaire $\rho_{V\otimes W}$, ie c'est un G-morphisme, $f \in Hom_G(V,W)$.

Définition 1.10. Caractères Soit ρ une représentation d'un groupe G sur V de dimension n. On lui associe son *caractère* χ_ρ défini par $\chi_\rho(s) = tr(\rho(s))$ où tr désigne la trace.

Proposition 1.9. Propriétés des caractères *On a les propriétés suivantes :*

(i) $\chi_\rho(1) = n$

(ii) $\forall s \in G$, $\chi_\rho(s^{-1}) = \overline{\chi_\rho(s)}$.

(iii) $\forall (s,t) \in G^2$, $\chi_\rho(tst^{-1}) = \chi_\rho(s)$ *: on dit que* χ_ρ *est une fonction centrale sur* G.

(iv) Si ρ *se décompose en une somme directe de deux représentations* ρ_V *et* ρ_W*, alors* $\chi_\rho := \chi_{V\oplus W} = \chi_{\rho V} + \chi_{\rho W}$.

(v) Si on note $\rho_{V\otimes W}$ *la représentation produit sur* $\mathcal{L}(V,W)$ *de deux représentations* ρ_V *et* ρ_W*, alors* $\rho_{V\otimes W} = \overline{\chi_{\rho V}}\chi_{\rho W}$.

Démonstration. (i) C'est évident car $tr(Id_V) = dim(V) = n$.

(ii) Vient du fait que l'on peut prendre une matrice unitaire pour $\rho(s)$ et de : $\chi_\rho(s^{-1}) = tr(\rho(s)^{-1}) = tr(\overline{\rho(s)}) = \overline{tr(\rho(s))}$.

(iii) Vient du fait que $\forall (A,B) \in GL_n(\mathbb{C})$, $tr(BAB^{-1}) = tr(A)$.

(iv) Si on note $\mathcal{B}_V$ une base de V et $\mathcal{B}_W$ une base de W, la matrice de $\rho_{V\oplus W}(s)$ s'écrit dans la base $\mathcal{B} := \mathcal{B}_V \cup \mathcal{B}_W$:

$$M(s) = \begin{pmatrix} M_V(s) & 0 \\ 0 & M_W(s) \end{pmatrix}$$

où $M_V(s)$ est la matrice de ρ_V(s) dans la base $\mathcal{B}_V$ et $M_W(s)$ celle de $\rho_W(s)$ dans $\mathcal{B}_W$. D'où $\chi_{V\oplus W}(s) = tr(M(s)) = tr(M_V(s)) + tr(M_W(s)) = \chi_V(s) + \chi_W(s)$.

(v) Provient du lemme suivant.

□

Lemme 1.10. *Soit* $u \in \mathcal{L}(W)$ *et* $v \in \mathcal{L}(V)$ *deux applications linéaires. On définit* $\Phi \in \mathcal{L}(\mathcal{L}(V),\mathcal{L}(W))$ *par la formule* $\Phi(f) = u \circ f \circ v$*, alors on a* $tr(\Phi) = tr(u)tr(v)$.

Démonstration. On se donne des bases $(e_i)_{i\in I}$ de V et $(f_j)_{j\in J}$ de W, ainsi que les bases duales $(e_i)^*_{i\in I}$ et $(f_j^*)_{j\in J}$. On peut construire une base $(F_{i,j})_{(i,j)\in I\times J}$ de $\mathcal{L}(V,W)$ par la formule :

$$\forall x \in V,\ F_{i,j}(x) := \langle e_i^*,x\rangle f_j \in W$$

La base duale est ainsi définie par la propriété :

$$\forall f \in \mathcal{L}(V,W),\ \langle F_{i,j}^*,f\rangle = \langle f_j^*,f(e_i)\rangle$$

On a donc :

$$\begin{aligned} tr(\Phi) &:= \sum_{(i,j)\in I\times J} \langle F_{i,j}^*,\Phi(F_{i,j})\rangle = \sum_{(i,j)\in I\times J} \langle f_j^*,u\circ F_{i,j}(v(e_i))\rangle \\ &= \sum_{(i,j)\in I\times J} \langle f_j^*,u(\langle e_i^*,v(e_i)\rangle f_j)\rangle = \sum_{(i,j)\in I\times J} \langle f_j^*,u(f_j)\rangle\langle e_i^*,v(e_i)\rangle = tr(u)tr(v) \end{aligned}$$

□

Définition 1.11. Produits hermitiens Si φ et ψ sont deux fonctions de G dans $\mathbb{C}$, on pose :

$$(\varphi,\psi) := \frac{1}{|G|}\sum_{t\in G} \varphi(t)\overline{\psi(t)}$$

$(.,.)$ est un *produit hermitien* sur l'espace vectoriel E des fonctions de G dans $\mathbb{C}$.

Théorème 1.11. Relations d'orthogonalité *Une famille de caractères de représentations irréductibles non deux à deux isomorphes forme une famille orthonormale de l'espace des fonctions de G dans $\mathbb{C}$, ce qui signifie :*

- *Si χ est le caractère d'une représentation irréductible, on a $(\chi,\chi) = 1$.*
- *Si χ et χ' sont deux caractères de représentations irréductibles non isomorphes, on a $(\chi,\chi') = 0$.*

Démonstration. Soient ρ_1 et ρ_2 deux représentations de la famille considérée, respectivement sur des espaces vectoriels V et W. Avec la proposition 1.8, on a donc : $tr(R_G) = \varepsilon$, où $\varepsilon = +1$ si les deux représentations sont isomorphes (donc en fait égales), et 0 sinon. Or :

$$tr(R_G) = \frac{1}{G}\sum_{s\in G} tr(\rho_{V\otimes W})(s) = \frac{1}{G}\sum_{s\in G} \chi_{\rho V\otimes W}(s)$$

Or on a vu à que $\chi_{V\otimes W}(s) = \overline{\chi_V(s)}\chi_W(s)$, donc on a bien :

$$tr(R_G) = \frac{1}{G}\sum_{s\in G} \overline{\chi_V(s)}\chi_W(s) := (\chi_W,\chi_V) = \varepsilon$$

□

Proposition 1.12. Unicité de la décomposition *On suppose qu'une représentation ρ de G sur V est décomposée en somme de représentations irréductibles $V = W_1 \oplus \ldots \oplus W_r$. Alors si W est une représentation irréductible de caractère χ_W, le nombre de fois que W intervient dans la décomposition (ie le nombre de W_i isomorphes à W) est indépendant de la décomposition et vaut (χ_ρ,χ_W). Au final, si on choisit une famille $(U_1,\ldots,U_r)$ de représentations deux à deux non isomorphes, on écrit de manière unique $V = n_1W_1 \oplus \ldots \oplus n_rW_r$ avec $n_i = (\chi_\rho,\chi_{W_i})$.*

Corollaire 1.13. *Deux représentations sont isomorphes si et seulement si elles ont même caractères. De plus, une représentation sur V de caractère χ_V est irréductible si et seulement si $(\chi_V,\chi_V) = \sum n_i^2 = 1$.*

Remarque. En fait, on peut montrer que famille des χ_{W_i} forme une base orthonormale de l'espace vectoriel des fonctions centrale. Le nombre de W_i est donc égal aux nombre de classes de conjugaisons dans G.

Référence : [Ser66, p.1][BR74, p.267]

Utilisation : (***,14) (**,2) (*,0)

Mots clefs : action de groupe, groupes finis, caractères, matrices semblables, sous-espaces stables, dimension, produit hermitien, espace hermitien, sous groupes finis de $SO(3)$.

100	Méthodes combinatoires, problèmes de dénombrement. Séries génératrices.	***
101	Groupe opérant sur un ensemble. Exemples et applications.	***
103	Sous-groupes distingués, groupes quotients. Exemples et 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 $GL(E)$. Applications.	***
107	Sous-groupes finis de $O(2,\mathbb{R})$, de $O(3,\mathbb{R})$. Applications.	***
118	Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.	***
119	Matrices équivalentes. Matrices semblables. Applications.	***
122	Réduction d'un endomorphisme en dimension finie. Applications.	***
123	Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.	***
126	Endomorphismes remarquables d'un espace vectoriel hermitien de dimension finie.	***
136	Formes linéaires sur un espace vectoriel de dimension finie. Espace dual, orthogonalité. Applications.	***
138	Endomorphismes diagonalisables.	***
105	Groupe des permutations d'un ensemble fini. Applications.	**
144	Utilisation des groupes en géométrie.	**

1.5 Action du groupe modulaire sur le demi plan de Poincarré

Référence : [Ale99, p.81]
Utilisation : (***,6) (**,0) (*,0)
Mots clefs : actions de groupe, homographies, partie génératrice, réseaux.

101	Groupe opérant sur un ensemble. Exemples et applications.	***
102	Sous-groupes discrets de $\mathbb{R}^n$. Réseaux.	***
130	Homographies de la droite complexe. Applications.	***
131	Applications des nombres complexes à la géométrie.	***
137	Exemples de parties génératrices d'un groupe.	***
144	Utilisation des groupes en géométrie.	***

1.6 Etude du groupe circulaire

Référence : [Aud98, p.152]
Utilisation : (***,1) (**,2) (*,0)
Mots clefs : homographies, droites et cercles, droite projective.

133	Exemples de propriétés projectives et d'utilisation d'éléments à l'infini.	***
130	Homographies de la droite complexe. Applications.	**
131	Applications des nombres complexes à la géométrie.	**

1.7 Applications conformes de la droite projective complexe

Référence : [Car61, p.182]
Utilisation : (***,4) (**,1) (*,0)
Mots clefs : homographies, angles, droite projective, fonctions holomorphes.

130	Homographies de la droite complexe. Applications.	***
132	Utilisation des angles en géométrie.	***
133	Exemples de propriétés projectives et d'utilisation d'éléments à l'infini.	***
143	Problèmes d'angles et de distances.	***
131	Applications des nombres complexes à la géométrie.	**

1.8 Invariants de similitude, version algébrique

Référence : [Gou94a, p.219]
Utilisation : (***,6) (**,0) (*,0)
Mots clefs : réduction d'endomorphismes, dualité, matrices semblables.

119	Matrices équivalentes. Matrices semblables. Applications.	***
122	Réduction d'un endomorphisme en dimension finie. Applications.	***
123	Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.	***
136	Formes linéaires sur un espace vectoriel de dimension finie. Espace dual, orthogonalité. Applications.	***
138	Endomorphismes diagonalisables.	***
141	Polynômes d'endomorphismes. Applications.	***

1.9 Invariants de similitude, version euclidienne

Référence : [Art91, p.450]
Utilisation : (***,1) (**,8) (*,0)
Mots clefs : réduction d'endomorphismes, dualité, modules, matrices semblables, division euclidienne.

120	Opérations élémentaires sur les lignes et les colonnes d'une matrice. Résolution d'un système d'équations linéaires. Applications.	***
102	Sous-groupes discrets de $\mathbb{R}^n$. Réseaux.	**
108	Congruences dans $\mathbb{Z}/n\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.	**
119	Matrices équivalentes. Matrices semblables. Applications.	**
122	Réduction d'un endomorphisme en dimension finie. Applications.	**
123	Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.	**
137	Exemples de parties génératrices d'un groupe.	**
138	Endomorphismes diagonalisables.	**
141	Polynômes d'endomorphismes. Applications.	**

1.10 Etude topologique de SO(3) via les quaternions

Référence : [MT97, p.125]
Utilisation : (***,4) (**,4) (*,0)
Mots clefs : inversion locale, quaternions, exponentielle, applications ouvertes, connexité.

125	Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie.	***
126	Endomorphismes remarquables d'un espace vectoriel hermitien de dimension finie.	***
131	Applications des nombres complexes à la géométrie.	***
139	Exponentielle de matrices. Applications.	***
130	Homographies de la droite complexe. Applications.	**
133	Exemples de propriétés projectives et d'utilisation d'éléments à l'infini.	**
141	Polynômes d'endomorphismes. Applications.	**
144	Utilisation des groupes en géométrie.	**

1.11 Champs équiprojectifs, application à la cinématique

Référence : [Gob95b, p.? (Chap.8)]
Utilisation : (***,1) (**,0) (*,0)
Mots clefs : vissage, produit vectoriel, isométries.

127	Isométries d'un espace affine euclidien de dimension finie. Formes réduites. Applications.	***

1.12 Existence de solution en programmation linéaire

Voici les principales étapes de l'exposé :

- On veut trouver $u$tel que $J(u) = \inf_{\mathcal{U}} J(v)$où $J(v) = (a,v)$, avec pour le problème original $\mathcal{U} = \{v \in \mathbb{R}^n;\ Cv \leq d\}$. On transforme ce problème en $(\mathcal{P}) : \mathcal{U} = \{v \in \mathbb{R}^n_+;\ Cv = d\}$.
- On démontre la CNS d'éxistence de minimum : $\inf_{\mathcal{U}} J(v)`\infty \Leftrightarrow (\mathcal{P})$a une solution. On utilise le fait que le cone positif engendré par les images de la base canonique par la matrice $\begin{pmatrix} a^T \\ C \end{pmatrix}$est fermé (cf. lemme de *Farkas-Minkowski*).
- On donne la CNS pour qu'un point de $\mathcal{U}$soit un sommet : on note C^jles colonnes de C, et donc $\mathcal{U} = \{v \in \mathbb{R}^n_+;\ \sum_{j=1}^n v_j C^j = d\}$. On note $I^*(v) = \{j = 1 \dots n;\ v_j \neq 0\}$. Le résultat important est que $v \in \mathcal{U}$est un sommet *ssi* les $\{C^j\}_{j \in I^*(u)}$sont libres.
- Comme corollaire, si $(\mathcal{P})$admet une solution, alors au moins un sommet est solution. Se fait par récurrence en diminuant la le nombre de colonne liées en se déplaçant "en ligne droite".
- Enfin, on démontre que si $\mathcal{U}$n'est pas vide, il possède au moins un sommet, ce qui conduit en fait à résoudre le problème de minimisation de $J(v,\widetilde{v}) = \sum_{i=1}^m \widetilde{v}_i$sur $\widetilde{\mathcal{U}} = \{(v,\widetilde{v}) \in \mathbb{R}^n_+ \times \mathbb{R}^m_+;\ Cv + \widetilde{v}\}$. Si $\mathcal{U}$n'est pas vide, le minimum, 0, est atteint par les $(u,0)$; $u \in \mathcal{U}$, et un sommet de cet ensemble est bien un sommet de $\mathcal{U}$.

Référence : [Cia90, p.230]
Utilisation : (***,2) (**,2) (*,0)
Mots clefs : polyèdre, rang de matrices, points extrémaux, convexité, algorithme du simplexe, algorithmes.

129	Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.	***
136	Formes linéaires sur un espace vectoriel de dimension finie. Espace dual, orthogonalité. Applications.	***
100	Méthodes combinatoires, problèmes de dénombrement. Séries génératrices.	**
118	Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.	**

1.13 Formes de Hankel et nombres de racines d'un polynôme

Référence : [Gan66, p.198]
Utilisation : (***,1) (**,4) (*,1)
Mots clefs : polynôme, formes quadratiques, rang de matrices, relations de Newton.

124	Formes quadratiques. Applications.	***
105	Groupe des permutations d'un ensemble fini. Applications.	**
115	Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications.	**
116	Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.	**
118	Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.	**
112	Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.	*

1.14 Quadriques et classes de similitudes

Définition 1.12. Les formes quadratiques étudiées On identifie $\mathbb{R}^4$ à $E = M(2,\mathbb{R})$. Le déterminant définit sur E une forme quadratique $q(A) = ad - bc$, où l'on a noté $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. C'est une forme quadratique non dégénérée de signature (2,2). L'autre forme quadratique est définie par $l(A) = tr(A^2) = a^2 + d^2 + 2bc$. C'est une forme quadratique non dégénérée de signature (3,1). Un autre cône important est celui des matrices impotentes, noté C_{nilp}. On notera $C^*_{nilp} = C_{nilp} - \{0\}$.

Proposition 1.14. Etude de $C(q)$ *Le cône isotrope pointé $C(q) - \{0\}$ de q est composé des matrices de rang 1. Un représentant de chaque classe peut être donné par $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ou par λP où $P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, suivant que la trace λ est nulle ou pas. La matrice N correspond à la classe de similitude C^*_{nilp}.*
L'équation de l'hyperplan tangent à $C(q)$ en un point A est $\{X \in E, \quad tr(AX) = tr(A)tr(X)\}$. Cet hyperplan coupe $C(q)$ suivant deux plans $P_1(A)$ et $P_2(A)$. Ces deux plans se rencontrent suivant la génératrice de $C(q)$ issue de A.

Proposition 1.15. Etude de P_1 et P_2 *Pour $X \in C(q)$, $P_1(X)$ est constitué des matrices ayant même noyau que X, et $P_2(X)$ des matrices ayant même image que X.*

Définition 1.13. Hyperplans affines On note $H_0 = \{A \in E, \quad tr(A) = 0\}$, qui est un hyperplan vectoriel de E. On note H_s l'hyperplan des matrices symétriques.
Les hyperplans affines correspondants à H_0 sont les $H_a = \{A \in E, \quad tr(A) = a\}$.

Proposition 1.16. Etude de $C(l)$ *Pour $A \in C(l)$, l'hyperplan tangent en A à $C(l)$ est $\tau^l_A = H(A) = \{X \in E, \quad tr(AX) = 0\}$.*

Proposition 1.17. Cones et hyperplans *Sur H_0, on a $l = -2q$ et $C(q) \cap H_0 = C(l) \cap H_0 = C_{nilp}$.*
De même, $C(q) \cap H_s$ est un vrai cône de $\mathbb{R}^3$. Par contre, on a $C(l) \cap H_s = \{0\}$.
Enfin, on a aussi $C(q) \cap C(l) = C_{nilp}$.

Proposition 1.18. Obtention des hyperboloïdes

- *Pour $a \in \mathbb{R}$, $H_a \cap C(q)$ est un hyperboloïde à une nappe.*
- *Pour $a \in \mathbb{R}$, $H_a \cap C(l)$ est un hyperboloïde à deux nappes.*

Proposition 1.19. Etude de certains polynômes *Pour $A \in E$ on pose :*

$$\Pi_1(X) = det(A - XI_2) \text{ et } \Pi_2(X) = tr((A - XI_2)^2)$$

Les racines (λ_1,λ_2) de Π_1 et (μ_1,μ_2) de Π_2 forment un carré, les diagonales joignant les racines du même polynôme. En particulier :

- *Les racines de Π_1 sont réelles si et seulement si celles de Π_2 sont complexes conjuguées.*
- *Les racines de Π_2 sont réelles si et seulement si celles de Π_1 sont complexes conjuguées.*

Théorème 1.20. Etude des classes de similitude *Soit $A \in E$ une matrice de valeurs propres α et β.*

- *Si les valeurs propres sont réelles et distinctes, la classe de similitude de A est une hyperboloïde à une nappe.*
- *Si les valeurs propres sont complexes conjuguées et distinctes, la classe de similitude de A est une hyperboloïde à deux nappes.*
- *Si les deux valeurs sont égales et la matrice non scalaire, la classe de similitude est un vrai cône de R^3 privé de son sommet.*
- *Si la matrice est scalaire, la classe de similitude est un point.*

Référence : [Mne97, p.217]
Utilisation : (***,2) (**,2) (*,0)
Mots clefs : matrices semblables, quadriques, cônes, matrices nilpotentes.

119	Matrices équivalentes. Matrices semblables. Applications.	***
124	Formes quadratiques. Applications.	***
128	Coniques.	**
140	Endomorphismes nilpotents.	**

1.15 Transformée de Fourier sur un groupe fini

Définition 1.14. Dual d'un groupe Soit G un groupe fini. Par définition, un caractère χ est un morphisme du groupe G dans le groupe multiplicatif $\mathbb{C}^*$. On note $\widehat{G}$ l'ensemble des caractères, et on l'appelle le dual de G. $\widehat{G}$ est un groupe pour la multiplication des applications, i.e. pour $(\chi_1,\chi_2) \in \widehat{G}^2$ on définit $(\chi_1\chi_2)(x) = \chi_1(x)\chi_2(x)$.

Proposition 1.21. *Soit G un groupe fini de cardinal n. Les éléments de $\widehat{G}$ sont en fait les morphismes de G dans le groupe des racines nièmes de l'unité.*

Définition 1.15. On note E l'ensemble des fonctions de G dans $\mathbb{C}$. C'est un espace vectoriel de dimension $n = Card(G)$ sur $\mathbb{C}$. Sur E on définit un produit scalaire hermitien, pour $(f,g) \in E^2$ par la formule :

$$\langle f,g\rangle = \sum_{g\in G} \overline{f(x)}g(x)$$

Où $\overline{y}$ désigne le conjugué de y.

Proposition 1.22. Dans le cas cyclique *Soit $G = \mathbb{Z}/p\mathbb{Z}$. Soit $\omega = e^{\frac{2\imath\pi}{p}}$. Tous les éléments de $\widehat{G}$ sont alors de la forme, pour $i \in \{0,\dots,n-1\}$:*

$$\chi_i : G \to \mathbb{C}^*$$
$$x \mapsto (\omega^i)^x = e^{\frac{2\imath\pi ix}{p}}$$

On a $G \simeq \widehat{G}$, et même plus fort, car $\widehat{G}$ forme une base orthogonale de E.

Proposition 1.23. Cas général *Soit G un groupe fini commutatif. Alors $\widehat{G}$ est une base orthogonale de E. On peut le voir via la décomposition des $\mathbb{Z}$-modules (i.e. des groupes abéliens) :*

$$G \simeq \mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r\mathbb{Z} \qquad (p_1, \ldots, p_r) \in (\mathbb{N}^*)^r$$

ou alors en montrant que pour tout caractère sur un sous groupe $H \subset G$ peut être prolonger en un caractère de G, ce qui induit la suite exacte : $\{1\} \to \widehat{G/H} \hookrightarrow \widehat{G} \twoheadrightarrow \widehat{H} \to \{1\}$ où la flèche $\widehat{G} \twoheadrightarrow \widehat{H}$ est le morphisme de restriction. Ceci montre que $\|\widehat{G}\| = \|\widehat{H}\|\|\widehat{G/H}\|$, et permet de démontrer par récurrence sur $\|G\|$ que $\|\widehat{G}\| = \|G\|$.

Remarque. Tout ceci est faux dans le cas non commutatif, comme le montre l'étude du groupe symétrique S_n. En effet, si on prend $f_1 = (a,b)$ et $f_2 = (c,d)$ deux transpositions, soit alors une permutation g dans S_n telle que : $g(a) = c$, $g(b) = d$. On a : $f_2 = g f_1 g^{-1}$ d'où , si on note χ un caractère :

$$\chi(f_2) = \chi(g f_1 g^{-1}) = \chi(g)\chi(f_1)\chi(g)^{-1} = \chi(f_1)$$

Donc χ est constante sur les transpositions, et comme $\chi(f_1^2) = \chi(f_1)^2 = 1$ on a $\chi(f_i) = +1$ ou $\chi(f_i) = -1$. Pour conclure, il suffit, si on prend une permutation quelconque f dans S_n, de la décomposer en produit de transpositions, et on a donc seulement deux caractères :

$$\forall f \in G, \chi_1(f) = 1 \quad \text{et}$$
$$\chi_2(f) = (-1)^{\varepsilon(f)}$$

Où ε désigne la signature. La solution pour contourner ce problème de « manque » de caractère est de considérer des représentations de notre groupe ainsi que les caractères de ces représentations (le dual est composé uniquement des caractères des représentations de dimension 1).

Référence : [Ser70, p.103][DMK72, p.203][War71, p.74][CLR92, p.764][Dem97, p.93]

Utilisation : (***,5) (**,2) (*,0)

Mots clefs : groupe fini, dualité, racines de l'unité, caractères, produit hermitien, transformée de Fourier, algorithmes, polynômes, racines de l'unité.

103	Sous-groupes distingués, groupes quotients. Exemples et applications.	***
104	Groupes finis. Exemples et applications.	***
108	Congruences dans $\mathbb{Z}/n\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.	***
114	Groupe des nombres complexes de module 1. Applications.	***
137	Exemples de parties génératrices d'un groupe.	***
126	Endomorphismes remarquables d'un espace vectoriel hermitien de dimension finie.	**
136	Formes linéaires sur un espace vectoriel de dimension finie. Espace dual, orthogonalité. Applications.	**

1.16 Transformée de Fourier discrète

Référence : [Dem97, p.93][Mal00, p.41]

Utilisation : (***,1) (**,1) (*,0)

Mots clefs : groupe fini, groupe cyclique, transformée de Fourier, algorithme FFT, équations aux dérivées partielles, équation de Poisson, calcul des coefficients de Fourier.

114	Groupe des nombres complexes de module 1. Applications.	***
108	Congruences dans $\mathbb{Z}/n\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.	**

1.17 Factorisation QR et méthode QR de recherche de valeurs propres

Référence : [Cia90, p.123]

Utilisation : (***,1) (**,1) (*,0)

Mots clefs : opérations élémentaires, factorisation de matrices, valeurs propres, itérations, algorithmes.

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

1.18 Décomposition de Jordan et applications

Référence :
Utilisation : (***,1) (**,0) (*,0)
Mots clefs : dualité, sous-espaces stables, exponentielle de matrices, systèmes différentiels linéaires.

140	Endomorphismes nilpotents.	***

1.19 Programmation convexe

Voici les principales étapes de l'exposé :

- Démonstration du lemme de Farkas : soient $\{a_1,\dots,a_n\}$et $n \in H$un Hilbert. On a : $\{(a_i,x) \leq 0;\ \forall i = 1\dots n\} \subset \{(b,x) \leq 0\} \Leftrightarrow b = \sum_{i=0}^{n} \lambda_i a_i \quad$ avec $\lambda_i \geq 0$.
- Définition du cône des directions admissibles en un point $u \in \mathcal{U}$, on montre qu'il est fermé, et que si une fonctionnelle Jadmet un minimum en u, alors $\forall v \in u + C(u)$, $J'(u)(v-u) \geq 0$.
- On se place dans le cas où l'ouvert est défini par $\mathcal{U} = \{v \in V;\ \forall i = 1\dots m,\ \varphi_i(v) \leq 0\}$. On note $I(u) = \{i;\ \varphi(u) = 0\}$et $C^*(u) = \{w \in V;\ \forall i \in I(u), (\varphi_i'(u),w) \leq 0\}$. On a toujours $C(U) \subset C^*(u)$.
- On donne une première définition de contraintes qualifiées : soit les $varphi_i$ pour $i \in I(u)$ sont affines, soit il existe un point $w \in V$ tel que $\varphi_i'(u)w \leq 0$ (avec inégalité stricte dans le cas affine). Dans ce cadre, on a $C(U) = C^*(u)$.
- On peut alors énoncer le théorème général de programmation non linéaire : si Jadmet un minimum en $u$et que les contraintes y sont qualifiées, alors il existe $\lambda_i(u) \geq 0$tels que $J'(u) + \sum_{i \in I(u)} \lambda_i(u)\varphi'(u) = 0$.
- Dans le cas où les contraintes sont convexes, on a une condition simple pour que les contraintes soient qualifiées (indépendantes du point). Ou bien toutes les $\varphi_i$sont affines et $\mathcal{U}$est non vide. Ou bien $\exists w \in \Omega \supset \mathcal{U}$tel que $\varphi(w) \leq 0$(avec inégalité stricte dans le cas affine).
- Enfin, on énonce les relations de *Kuhn et Tucker* dans le cas des contraintes convexes, qui renforce sous la forme d'une CNS la relation déjà énoncée pour la programmation non linéaire.

Référence : [Cia90, p.207]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : convexité, fonctions convexes, calcul différentiel, cône convexe, séparation des convexes.

129	Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.	**

1.20 Théorème de l'angle pivotant

Référence : [LB88, p.69]
Utilisation : (***,4) (**,0) (*,0)
Mots clefs : coniques, angles, règle et compas.

128	Coniques.	***
132	Utilisation des angles en géométrie.	***
134	Constructions à la règle et au compas.	***
143	Problèmes d'angles et de distances.	***

1.21 Algorithme de Berlekamp

Référence : [Dem97, p.215][AB93, p.100][Mig89, p.262]
Utilisation : (***,5) (**,1) (*,0)
Mots clefs : corps fini, polynômes irréductibles, algorithmes, rang de matrices.

109	Nombres premiers. Applications.	***
111	Corps finis. Applications.	***
113	Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.	***
116	Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.	***
118	Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.	***
108	Congruences dans $\mathbb{Z}/n\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.	**

1.22 Bases de Gröbner

Voici les principales choses à dire sur ce sujet :

- Ordre sur les monômes d'un polynômes, le monôme de tête noté LT(f). Algorithme de division, problème : on n'obtient pas toujours de reste nuls pour les polynômes de l'idéal !
- Définition des bases de Gröbner : $\{g_1,\ldots,g_n\}$ est une base de Gröbner de l'idéal I *ssi* $\{LT(g_1),\ldots,LT(g_n)\}$ engendre $LT(I)$. Quand on divise par une base de Gröbner, le reste est nul ssi le polynôme fait parti de l'idéal. De plus on a unicité du reste.
- Présentation de l'algorithme de *Buchberger*, via l'introduction du polynôme-S :

$$(f_1,f_2) = \frac{x^\gamma}{LT(f_1)} f1 - \frac{x^\gamma}{LT(f_2)} f2$$

où x^γ est le plus petit monôme divisible par $LT(f_1)$ et $LT(f_2)$. Base de Gröbner réduite.
- Utilisation des bases de Gröbner pour l'élimination. Si on prend $I \subset k[x_1,\ldots,x_n]$ un idéal dont $G == \{f_1,\ldots,f_t\}$ est une base de Gröbner pour l'ordre lexical $x_n \prec \ldots \prec x_n$, alors pour $k = 2\ldots n$, l'ensemble $G \cap k[x_k,\ldots,x_n]$ est une base de Gröbner de l'idéal d'élimination $I \cap k[x_k,\ldots,x_n]$. Le problème est de savoir si on peut "remonter", i.e. si une solution du système $I \cap k[x_n]$ peut se relever en une solution du système $I \cap k[x_{n-1},x_n]$, etc. La réponse est positive sur $k = \mathbb{C}$ (théorème d'extension).
- Applications des bases de Gröbner. Par exemple, on peut montrer que la variété affine $V(I) \subset \mathbb{C}^n$ est vide *ssi* $I = \mathbb{C}[x_1,\ldots,x_n]$ *ssi* $\{1\}$ est une base de Gröbner réduite de I. Ceci permet de décider si un graphe peut être colorié avec 3 couleurs, en ajoutant l'équation $x_i^3 - 1 = 0$ pour chaque sommet i (les couleurs sont les racines cubiques de 1), et pour chaque arrête (i,j) l'équation $x_i^2 + x_i x_j + x_j^2 = 0$. On peut aussi citer l'utilisation de bases de Gröbner pour résoudre les équations polynomiales résultant de la cinématique inverse pour les robots articulés.

Référence : [CLO96, p.48][CS97, p.1]
Utilisation : (***,2) (**,0) (*,0)
Mots clefs : idéal, polynômes, algorithmes, équations polynomiales, élimination.

110	Idéaux d'un anneau commutatif unitaire. Exemples et applications.	***
115	Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications.	***

1.23 Codes correcteurs linéaires cycliques

Référence : [Dem97][PH89, p.151][PW95, p.1]
Utilisation : (***,7) (**,12) (*,0)
Mots clefs : polynôme, idéal, dualité, réseau, dénombrement, cyclotomie, relations de Newton, division euclidienne.

100	Méthodes combinatoires, problèmes de dénombrement. Séries génératrices.	***
108	Congruences dans $\mathbb{Z}/n\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.	***
109	Nombres premiers. Applications.	***
110	Idéaux d'un anneau commutatif unitaire. Exemples et applications.	***
111	Corps finis. Applications.	***
113	Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.	***
116	Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.	***
101	Groupe opérant sur un ensemble. Exemples et applications.	**
102	Sous-groupes discrets de $\mathbb{R}^n$. Réseaux.	**
105	Groupe des permutations d'un ensemble fini. Applications.	**
114	Groupe des nombres complexes de module 1. Applications.	**
115	Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications.	**
117	Équations diophantiennes du premier degré $ax + by = c$. Exemples d'équations diophantiennes de degré supérieur.	**
118	Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.	**
120	Opérations élémentaires sur les lignes et les colonnes d'une matrice. Résolution d'un système d'équations linéaires. Applications.	**
123	Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.	**
133	Exemples de propriétés projectives et d'utilisation d'éléments à l'infini.	**
136	Formes linéaires sur un espace vectoriel de dimension finie. Espace dual, orthogonalité. Applications.	**
137	Exemples de parties génératrices d'un groupe.	**

1.24 Sous groupes finis de SO(3)

Référence : [BR74]
Utilisation : (***,1) (**,3) (*,0)
Mots clefs : groupes finis, isométries, action de groupe, équation aux classes.

107	Sous-groupes finis de $O(2,\mathbb{R})$, de $O(3,\mathbb{R})$. Applications.	***
100	Méthodes combinatoires, problèmes de dénombrement. Séries génératrices.	**
101	Groupe opérant sur un ensemble. Exemples et applications.	**
104	Groupes finis. Exemples et applications.	**

1.25 2ème théorème de Poncelet

Référence : [?]
Utilisation : (***,1) (**,4) (*,0)
Mots clefs : racines de polynôme, coniques, angles, règle et compas.

128	Coniques.	***
116	Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.	**
131	Applications des nombres complexes à la géométrie.	**
132	Utilisation des angles en géométrie.	**
143	Problèmes d'angles et de distances.	**

1.26 Nombres constructibles à la règle et au compas

Référence : [Car89, p.1]
Utilisation : (***,1) (**,3) (*,3)
Mots clefs : extensions de corps, polynômes irréductibles, cyclotomie, règle et compas.

134	Constructions à la règle et au compas.	***
113	Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.	**
131	Applications des nombres complexes à la géométrie.	**
143	Problèmes d'angles et de distances.	**
109	Nombres premiers. Applications.	*
114	Groupe des nombres complexes de module 1. Applications.	*
132	Utilisation des angles en géométrie.	*

1.27 Courbes rationnelles

Référence : [Gob95a][Per95, p.6]
Utilisation : (***,4) (**,1) (*,0)
Mots clefs :

112	Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.	***
115	Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications.	***
117	Équations diophantiennes du premier degré $ax + by = c$. Exemples d'équations diophantiennes de degré supérieur.	***
121	Déterminant. Applications.	***
110	Idéaux d'un anneau commutatif unitaire. Exemples et applications.	**

1.28 Corps finis et théorème de Chevalley

Référence : [Sam67, p.29]
Utilisation : (***,1) (**,2) (*,0)
Mots clefs : corps finis, polynôme.

117	Équations diophantiennes du premier degré $ax + by = c$. Exemples d'équations diophantiennes de degré supérieur.	***
111	Corps finis. Applications.	**
115	Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications.	**

1.29 Groupes à paramètres d'automorphismes

Référence : [Car97, p.142][MT97, p.63][Arn74, p.59]
Utilisation : (***,1) (**,1) (*,0)
Mots clefs : groupes linéaire, calcul différentiel, convolution, équations différentielles, espace des flots.

139	Exponentielle de matrices. Applications.	***
106	Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.	**

1.30 Résultant et application à l'élimination

Soient $f(X) = \sum_{i=0}^{m} a_i X^i$et $g(X) = \sum_{i=0}^{n} a_i X^i$deux polynômes sur un corps $\mathbb{K}$. Lorsque $f$et $g$possèdent un facteur non trivial, ie. $f = f_1 h$et $g = g_1 h$, l'équation :

$$uf + vg = 0 \quad \text{avec } \deg(u) \leq \deg(g) - 1 \text{ et } \deg(v) \leq \deg(f) - 1 \tag{2}$$

possède les solutions $u = g_1$et $v = -f_1$. Réciproquement, l'existence de solution nulle implique l'existence d'un facteur commun non trivial. En projetant l'équation (2) sur la base canonique de $\mathbb{K}_m[X] \times \mathbb{K}_n[X]$, l'existence

de solution non nulle est équivalente à la nullité du déterminant :

$$\begin{vmatrix} a_m & & & & b_n & & & \\ a_{m-1} & a_m & & & b_{n-1} & b_n & & \\ & a_{m-1} & \ddots & & & b_{n-1} & \ddots & \\ \vdots & & \ddots & a_m & \vdots & & \ddots & b_n \\ a_0 & \vdots & & a_{m-1} & b_0 & \vdots & & b_{n-1} \\ & a_0 & & & & b_0 & & \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & a_0 & & & & b_0 \end{vmatrix} \tag{3}$$

Définition 1.16. Le déterminant (3) se nomme le résultant de $f$et $g$et se note $Res_X(f,g)$.

Théorème 1.24. Propriétés du résultant

(i) $Res_X(f,g) = (-1)^{mn} Res_X(g,f)$

(ii) $Res_X(f,b_0) = b_0^m$, *pour* $b_0 \in \mathbb{K}$.

(iii) *Si* $\deg(f) = m \leq n = \deg(g)$, *et si* h *est le reste de la division de* g*par* f, *on a* $Res_X(f,g) = a_m^{n-m} Res_X(f,h)$.

(iv) $Res_X(f,g) = 0$*si et seulement si* f*et* g*ont un facteur non trivial.*

(v) *Si* f *et* g *s'écrivent :*

$$f = a_0(X-\alpha_1)(\ldots)(X-\alpha_m) \tag{4}$$
$$g = b_0(X-\beta_1)(\ldots)(X-\beta_n) \tag{5}$$

alors on a :

$$Res_X(f,g) = a_m^n \prod_{i=1}^{m} g(\alpha_i) = (-1)^{mn} b_n^m \prod_{j=1}^{n} f(\beta_j) = a_m^n b_n^m \prod_{i=1}^{m}\prod_{j=1}^{n} (\alpha_i - \beta_j)$$

Remarque. Si on se place dans la clôture algébrique $\overline{\mathbb{K}}$ de $\mathbb{K}$, alors l'écriture (4) est toujours réalisée et on peut appliquer (v).

Proposition 1.25. Généralisation *Le résultant est un polynôme entier en les coefficient de* f *et* g, *i.e.* $Res_X(f,g) \in \mathbb{Z}[a_0,\ldots,a_m,b_0,\ldots,b_m]$. *Ceci permet de le calculer dans un anneau* A *quelconque.*
Si l'anneau A *est intègre et factoriel, en utilisant le théorème précédent dans le corps de fraction* $Frac(A)$, *on garde la propriété que* f *et* g *on un facteur commun non trivial si et seulement si* $Res_X(f,g) = 0$, *ce qui est équivalent à une racine commune dans une extension algébriquement close de* A.

Remarque. La proposition 1.25 nous permet de traiter le cas des polynômes en plusieurs variables, i.e. si $f \in \mathbb{K}[X_1,\ldots,X_n]$, on utilise $f \in A[X_n]$ avec $A = \mathbb{K}[X_1,\ldots,X_{n-1}]$ qui est intègre et factoriel.

On souhaite éliminer la variable X_r entre deux polynômes $f,g \in \mathbb{K}[X_1,\ldots,X_r]$, notés de la façon suivante :

$$f = \sum_{i=0}^{m} f_i X_r^i \qquad f_i \in \mathbb{K}[X_1,\ldots,X_{r-1}] \qquad f_m \neq 0 \tag{6}$$
$$g = \sum_{i=0}^{n} g_i X_r^i \qquad g_i \in \mathbb{K}[X_1,\ldots,X_{r-1}] \qquad g_n \neq 0 \tag{7}$$

Définition 1.17. Idéal d'élimination Pour $f \in \mathbb{K}[X_1,\ldots,X_r]$, on note $f(\alpha_1,\ldots,\alpha_r)$ le polynôme évalué en $(\alpha_1,\ldots,\alpha_r) \in \overline{\mathbb{K}}^r$. On pose $h = Res_{X_r}(f,g) \in \mathbb{K}[X_1,\ldots,X_{r-1}]$. Soit $I = \langle f,g \rangle$. On note $I_r = I \cap \mathbb{K}[X_1,\ldots,X_{r-1}]$. C'est l'idéal d'élimination. En quelque sorte, l'idéal I_r contient toutes les façons d'éliminer la variable X_r des équations $\{f = 0, g = 0\}$.

Proposition 1.26. ELIMINATION *On a $h \in I_r$. Donc si $(\alpha_1,\dots,\alpha_r) \in \overline{\mathbb{K}}^r$ est un zéro commun de f et g, alors $h(\alpha_1,\dots,\alpha_{r-1}) = 0$. Au final, le calcul de h conduit à une équation en $r-1$ variables.*

Théorème 1.27. EXTENSION *On suppose connu $(\alpha_1,\dots,\alpha_{r-1}) \in \overline{\mathbb{K}}^{r-1}$ tels que $h(\alpha_1,\dots,\alpha_{r-1}) = 0$. Alors, si on n'est pas dans l'un des cas suivants :*

- $\forall i \in \{0,\dots,m\}$, $f_i(\alpha_1,\dots,\alpha_{r-1}) = 0$
- $\forall i \in \{0,\dots,n\}$, $g_i(\alpha_1,\dots,\alpha_{r-1}) = 0$
- $f_m(\alpha_1,\dots,\alpha_{r-1}) = g_n(\alpha_1,\dots,\alpha_{r-1}) = 0$

il existe $\alpha_r \in \overline{\mathbb{K}}$ tel que $(\alpha_1,\dots,\alpha_r)$ soit un zéro commun à f et g.

Référence : [CLO96, p.147][CS97, p.25][Mig89, p.162]
Utilisation : (***,0) (**,3) (*,0)
Mots clefs : déterminant, polynômes, équations polynomiales, élimination.

115	Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications.	**
116	Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.	**
121	Déterminant. Applications.	**

1.31 Polynômes orthogonaux

Référence : [Dem96, p.51]
Utilisation : (***,1) (**,0) (*,0)
Mots clefs : polynômes orthogonaux, espace L^2, polynôme de meilleure approximation.

135	Polynômes orthogonaux. Applications.	***

1.32 Forme réduite d'une application affine

Référence : [Aud98, p.23]
Utilisation : (***,1) (**,0) (*,0)
Mots clefs : isométrie, espace affine.

127	Isométries d'un espace affine euclidien de dimension finie. Formes réduites. Applications.	***

1.33 Méthodes de Gauss et polynômes orthogonaux

Définition 1.18. ESPACE FONCTIONNEL Soit $w :]\alpha,\beta[\to \mathbb{R}_+^*$ une fonction continue telle que $\forall n, \int_\alpha^\beta |x|^n w(x)dx < \infty$. On considère l'espace vectoriel E des fonctions de module carré intégrable pour le poids $w(x)$, muni du produit scalaire :

$$\langle f,g \rangle = \int_\alpha^\beta f(x)g(x)w(x)dx$$

Théorème 1.28. POLYNÔMES ORTHOGONAUX *Il existe une unique suite $\{p_n\}_{n\in\mathbb{N}}$ de polynômes unitaires deux*

à deux orthogonaux pour $\langle .,. \rangle$. De plus, ces polynômes sont donnés par la relation de récurrence :

$$p_n(x) = (x - \lambda_n)p_{n-1}(x) - \mu_n p_{n-2}(x) \quad \textit{avec :}$$
$$\lambda_n = \frac{\langle xp_{n-1}, p_{n-1}\rangle}{\|p_{n-1}\|^2} \quad \textit{et :}$$
$$\mu_n = \frac{\|p_{n-1}\|^2}{\|p_{n-2}\|^2}$$

Enfin, p_n a n racines simples distinctes dans $]a,b[$.

Théorème 1.29. Méthode de Gauss *On cherche une formule approchée de la forme :*

$$\int_\alpha^\beta f(x)w(x)dx \simeq \sum_{j=0}^{l} \lambda_j f(x_j) \text{ pour } x_j \in [\alpha,\beta]$$

Il existe un choix et un seul des points x_j et des poids λ_j de sorte que la méthode soit d'ordre $N = 2l + 1$. Les points x_j sont alors les racines du $(l + 1)$-ième polynôme orthogonal pour le poids w sur $]\alpha,\beta[$.

Remarque. Les méthodes sont très puissantes à la fois parce qu'elles ont un ordre élevé, mais aussi parcequ'elle intègrent directement un poids w qui peut par exemple présenter des singularités sur le bord de l'intervalle. La seule restriction est de devoir calculer au préalable les racines des polynômes orthogonaux correspondants.

Remarque. Explication de la démarche Pour comprendre pourquoi est-ce que l'on est amené à choisir les zéros des polynômes orthogonaux comme points d'interpolation, il faut étudier de plus près la formule d'erreur correspondant à la méthode issue du choix de $N+1$ points d'interpolation : Si on note P_N le polynôme d'interpolation de f aux points $x_0 < \ldots < x_N$, alors, on peut utiliser les différences divisées définies de la manière suivante :

$$f[x_i] = f(x_i) \tag{8}$$
$$f[x_0,\ldots,x_k] = \frac{f[x_1,\ldots,x_k] - f[x_0,\ldots,x_{k-1}]}{x_k - x_0} \tag{9}$$

on a alors une expression du polynôme d'interpolation de *Lagrange* :

$$p_n(x) = \sum_{k=1}^{n} f[x_0,\ldots,x_k]\pi_k(x) \quad \text{avec :} \tag{10}$$
$$\pi_k(x) = (x - x_0)(x - x_1)\ldots(x - x_k) \tag{11}$$

et surtout un résultat fondamental :

$$f(x) - P_N(x) = f[x_0,\ldots,x_N,x]\pi_N(x) \tag{12}$$

En effet, avec le théorème de *Rolle*, ceci permet d'affirmer que :

$$\exists \xi_x \in]\alpha,\beta[,\ f(x) - P_n(x) = \frac{f^{(N+1)}(\xi_x)}{(N+1)!}\pi_N(x), \quad \text{d'où} \tag{13}$$
$$E(f) = \int_\alpha^\beta (f(x) - P_N(x))dx = \frac{1}{(N+1)!}\int_\alpha^\beta f^{(N+1)}(\xi_x)\pi_N(x)dx \tag{14}$$

Tout ces calculs permettent, entre autre, de démontrer les vitesses de convergence pour les méthodes de *Newton-Cotes*. Cependant, ils permettent aussi et surtout d'élaborer des méthodes plus performantes par la remarque suivante : si le polynôme π_N est tel que $\int_\alpha^\beta \pi_N(t)dt = 0$, alors, si on introduit un nouveau point de subdivision x_{N+1}, on peut exploiter la formule des différences divisées :

$$f[x_0,\ldots,x_N,x] = f[x_0,\ldots,x_N,x_{N+1}] + (x - x_{N+1})f[x_0,\ldots,x_N,x_{N+1},x] \tag{15}$$

ce qui permet d'augmenter l'ordre de la méthode, grace à la formule :

$$E(f) = \int_\alpha^\beta f[x_0,\ldots,x_N,x]\pi_N(x)dx \tag{16}$$

$$= \int_\alpha^\beta f[x_0,\ldots,x_N,x_{N+1},x]\pi_{N+1}(x)dx \tag{17}$$

Maintenant, il suffit de remarquer que si l'on a pu choisir le point x_{N+1} tel que $\int_\alpha^\beta \pi_{N+1}(t)dt = 0$, alors on peut recommencer ! Et jusqu'ou peut on aller ? Et bien le choix optimal est celui tel que le polynôme π_N qui correspond aux choix des $N+1$ premiers points (ceux qui détermine la méthode) soit orthogonaux aux polynômes "ajoutés", ie les $\prod_{i=N+1}^{N+k}(x-x_i)$. Ceci signifie donc que notre polynôme π_N doit être orthogonaux aux plus possible d'espaces E_{N+k} des polynômes de degré inférieur à $n+k$. Donc le choix optimal est celui des polynômes orthogonaux de *Legendre*, qui sont orthogonaux à tous les polynômes de degré inférieur à N. Bien sûr ce raisonnement marche aussi avec des intégrales comportant un poids w, ce qui conduit aux polynômes orthogonaux pour le poids utilisé.

Référence : [Dem96, p.50 et 73]

Utilisation : (***,0) (**,1) (*,0)

Mots clefs : polynômes, intégration numérique, vitesse de convergence, algorithmes, singularités, méthodes de quadratures.

135	Polynômes orthogonaux. Applications.	**

1.34 Fractions continues

Voici les principales choses à dire sur ce sujet :

- Qualité d'approximation d'un réel ξpar des rationnels : il existe une infinité de couples $(p,q) \in \mathbb{Z}\times\mathbb{N}^*$tels que $|\xi - \frac{p}{q}| \leq \frac{1}{q^2}$. comme utilisation des ce résultat, on peut citer le critère pour qu'un nombre impair soit somme de deux carrés : il suffit qu'il soit congru à 1 modulo 4.
- Qualité d'approximation de nombre algébrique : soit ξun nombre irrationnel algébrique de degrés $n$sur $\mathbb{Z}$. Alors pour tout εstrictement positif, l'inégalité $|\xi - \frac{p}{q}| \leq \frac{1}{q^{n+\varepsilon}}$n'admet qu'un nombre fini de solutions $(p,q) \in \mathbb{Z}\times\mathbb{N}^*$. Ceci permet de construire les nombres de Liouville : $\sum_{k\geq 1} a^{k!}$, qui sont transcendants pour tout entier a.
- On défini ensuite la notion de fraction réduite d'un nombre réel ξ, qui se dit d'une fraction réalisant, pour tous les dénominateurs plus petits, la meilleure approximation. On donne les formules de récurrence pour déterminer les réduites, ce qui abouti aux fractions continues.
- Comme application, on peut citer la résolution de l'équation de Pell : $x^2 - dy^2 = k$. On utilise le résultat suivant : l'équation $x^2 + dy^2 = \pm 1$admet en plus de la solution $(\pm 1,0)$une infinité de solutions $(\pm x_n, \pm y_n)$avec $x_n \geq > 0, y_n \geq 0$. On note (x_1,y_1)la solution telle que $x+y\sqrt{d}$soit minimal. On a alors $x_n+y_n\sqrt{d} = (x_1+y_1\sqrt{d})^n$. De plus, le développement en fraction continue de $\sqrt{d}$est périodique de période s, et le dernier quotient de cette période est (x_1,y_1). Enfin, on a $x_n^2 + dy_n^2 = (-1)^{ns}$

Référence : [Gou94a, p.87][Dem97, p.180][Des86, p.9]

Utilisation : (***,0) (**,3) (*,0)

Mots clefs : approximation des nombres réels, algorithme d'Euclide, division euclidienne, équations diophantiennes.

112	Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.	**
116	Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.	**
117	Équations diophantiennes du premier degré $ax + by = c$. Exemples d'équations diophantiennes de degré supérieur.	**

1.35 Isométries du demi plan hyperbolique

Référence : [Ale99, p.182]
Utilisation : (***,0) (**,3) (*,0)
Mots clefs : homographies, isométrie, droite projective.

130	Homographies de la droite complexe. Applications.	**
131	Applications des nombres complexes à la géométrie.	**
143	Problèmes d'angles et de distances.	**

1.36 Etude de l'exponentielle de matrice

Référence : [MT97, p.57]
Utilisation : (***,1) (**,3) (*,1)
Mots clefs : groupe linéaire, inversion locale, matrices nilpotentes.

140	Endomorphismes nilpotents.	***
139	Exponentielle de matrices. Applications.	**
140	Endomorphismes nilpotents.	**
141	Polynômes d'endomorphismes. Applications.	**
122	Réduction d'un endomorphisme en dimension finie. Applications.	*

1.37 Fonctions matricielles

Référence : [Gan66]
Utilisation : (***,0) (**,1) (*,2)
Mots clefs : interpolation, polynôme Lagrange.

139	Exponentielle de matrices. Applications.	**
122	Réduction d'un endomorphisme en dimension finie. Applications.	*
141	Polynômes d'endomorphismes. Applications.	*

1.38 Algorithmes gloutons sur un matroïde pondéré

Référence : [CLR92, p.338]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : extémas, optimisation.

100	Méthodes combinatoires, problèmes de dénombrement. Séries génératrices.	**

1.39 Progammation linéaire et plus court chemin

Référence : [CLR92, p.528]
Utilisation : (***,0) (**,0) (*,1)
Mots clefs : programmation linéaire, parcours de graphes, optimisation.

100	Méthodes combinatoires, problèmes de dénombrement. Séries génératrices.	*

1.40 Théorème du point fixe sur un treillis complet

Référence : [Dub53, p.38]
Utilisation : (***,0) (**,0) (*,0)
Mots clefs : treillis, point fixe, suite récurrente, itérations.

[pas de leçon l'utilisant]

1.41 Théorème des zéros de Hilbert

Référence : [Gob95b, p.230][Per95, p.16]
Utilisation : (***,3) (**,0) (*,0)
Mots clefs : polynômes, idéal, variétés algébriques, équations polynomiales, fractions rationnelles, dénombrabilité.

110	Idéaux d'un anneau commutatif unitaire. Exemples et applications.	***
112	Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications.	***
115	Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications.	***

1.42 Présentation du crytosystème RSA

Référence : [Gou94a, p.35]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : nombres premiers, factorisation, algorithmes, corps finis.

109	Nombres premiers. Applications.	**

1.43 Quelques tests de primalité

Référence : [Gou94a, p.36][Mig89, p.83][Dem97, p.72]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : nombres premiers, corps finis, symbole de Legendre, algorithmes.

109	Nombres premiers. Applications.	**

1.44 Le théorème de Tchebitcheff sur les nombres premiers

Référence : [Gou94a, p.43]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : nombres premiers, comportement asymptotique.

109	Nombres premiers. Applications.	**

1.45 Simplicité de $PSL_n(Z)$

Référence : [Per96, p.??]
Utilisation : (***,1) (**,2) (*,0)
Mots clefs : partie génératrice, groupe linéaire.

120	Opérations élémentaires sur les lignes et les colonnes d'une matrice. Résolution d'un système d'équations linéaires. Applications.	***
103	Sous-groupes distingués, groupes quotients. Exemples et applications.	**
137	Exemples de parties génératrices d'un groupe.	**

1.46 Base d'Auerbach

Référence : [ZQ95, p.160]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : déterminant, orthogonalité, optimisation, compacité.

121	Déterminant. Applications.	**

1.47 Algorithme LLL et factorisation de polynômes

Référence : [Mig89, p.318]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : polynômes, algorithme, réseaux.

102	Sous-groupes discrets de $\mathbb{R}^n$. Réseaux.	**

1.48 Champs de forces conservatifs, exemple du double pendule

Référence : [Arn76]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : équations différentielles, formes quadratiques.

124	Formes quadratiques. Applications.	**

1.49 Etude du mouvement des planètes

Référence : [Arn76, p.39]
Utilisation : (***,0) (**,2) (*,0)
Mots clefs : équations différentielles, coniques, courbes.

124	Formes quadratiques. Applications.	**
128	Coniques.	**

1.50 Borne inférieure de l'information

Référence : [CLR92]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : arbres binaires, combinatoire, algorithme.

100	Méthodes combinatoires, problèmes de dénombrement. Séries génératrices.	**

1.51 Séries génératrices, nombres de relations d'équivalences

Référence : [FGS90, p.518]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : combinatoire, séries entières.

100	Méthodes combinatoires, problèmes de dénombrement. Séries génératrices.	**

1.52 Etude des polyèdres réguliers

Référence : [Aud98]
Utilisation : (***,0) (**,0) (*,0)
Mots clefs : combinatoire, convexité, équation aux classes, barycentre.

[pas de leçon l'utilisant]

1.53 Etude de la croissance des groupes abéliens

Voici les principales choses à dire sur ce sujet :

- on commence par définir une relation d'équivalence sur les suites croissantes : $f \sim g \Leftrightarrow \exists(A,N_A) \in (N^*)^2, \forall N \geq N_A, f(N) \leq g(AN)$ et $g(N) \leq f(AN)$.
- Pour une partie génératrice Sd'un groupe abélien G, on note $l_S(x) = \min\{p \geq 1;\ \exists(s_1,\ldots,s_p) \in S^p$ tels que $x = s_1 \ldots s_p\}$. On défini alors $G_N = \{x \in G;\ l_S(x) \leq N\}$et $\gamma_S(N) = card(G_N)$, qui est la fonction de croissance du groupe. On vérifie en effet que la classe de croissance (exponentielle, polynomiale ...) ne dépend pas de S.
- On donne les exemples de $\mathbb{Z}^p$qui est à croissance polynomiale d'ordre p, et de $PSL_2(\mathbb{Z})$qui est à croissance exponentielle.
- On parle de métrique des mots, définie par $d_S(x,y) = l_S(xy^{-1})$, de graphe de Cayley (un arc est présent entre deux éléments x,$y$du groupe dés que $xy^{-1} \in S$), et de séries génératrices associées : $f(x) = \sum \gamma_S(n)x^n$.

Référence : [Ale99, p.90]
Utilisation : (***,0) (**,2) (*,0)
Mots clefs : groupes, combinatoire, comportement asymptotique, plan hyperbolique, parties génératrices.

100	Méthodes combinatoires, problèmes de dénombrement. Séries génératrices.	**
137	Exemples de parties génératrices d'un groupe.	**

1.54 Idéaux fermés de C(E)

Référence : [Gob95a, p.77]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : idéaux, topologie, compacité.

110	Idéaux d'un anneau commutatif unitaire. Exemples et applications.	**

1.55 Dualité entre les compacts, application aux polyèdres

Référence : [Gob95b]
Utilisation : (***,0) (**,2) (*,0)

Mots clefs : dualité, polyèdres.

129	Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.	**
136	Formes linéaires sur un espace vectoriel de dimension finie. Espace dual, orthogonalité. Applications.	**

1.56 Théorie de Galois et résolubilité

Référence : [Goz97]
Utilisation : (***,0) (**,4) (*,0)
Mots clefs : groupes finis, groupes symétrique, polynôme, racines de polynômes.

103	Sous-groupes distingués, groupes quotients. Exemples et applications.	**
105	Groupe des permutations d'un ensemble fini. Applications.	**
113	Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.	**
116	Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.	**

1.57 Groupes de pavage

Référence : [**?**]
Utilisation : (***,0) (**,4) (*,0)
Mots clefs : groupes, isométries, action de groupe.

107	Sous-groupes finis de $O(2,\mathbb{R})$, de $O(3,\mathbb{R})$. Applications.	**
127	Isométries d'un espace affine euclidien de dimension finie. Formes réduites. Applications.	**
132	Utilisation des angles en géométrie.	**
143	Problèmes d'angles et de distances.	**

1.58 Théorème de Dirichlet, version faible

Référence : [Goz97]
Utilisation : (***,0) (**,2) (*,0)
Mots clefs : congruence, nombres premiers, cyclotomie.

109	Nombres premiers. Applications.	**
114	Groupe des nombres complexes de module 1. Applications.	**

1.59 Critère de Routh

Théorème 1.30. Critère de Routh *Soit $f(z) = p_n z^n + \ldots + p_1 z + p_0$ un polynôme à coefficient réels avec $p_0 > 0$. Pour $i \in \{1,\ldots,n\}$ on considère les déterminants de taille i :*

$$D_i(f) = \begin{bmatrix} p_1 & p_0 & 0 & 0 & \ldots & 0 \\ p_3 & p_2 & p_1 & 0 & \ldots & 0 \\ p_5 & p_4 & p_3 & p_2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{2i-1} & p_{2i-2} & p_{2i-3} & p_{2i-4} & \vdots & p_i \end{bmatrix}$$

où l'on a posé $p_i = 0$ si $i > n$. Alors toutes les racines de f sont de partie réelle strictement négatives ***si et seulement si*** *$\forall i \in \{1,\ldots,n\}, D_i(f) > 0$.*

Référence : [Mig89, p.223][Gan66, p.167]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : polynômes, racines de polynômes, localisation, équations différentielles.

116	Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.	**

1.60 Théorème de Fermat pour n=3 ou pour n=2/n=4

Référence : [Sam67]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : polynômes, racines de polynômes, équations diophantiennes.

117	Équations diophantiennes du premier degré $ax + by = c$. Exemples d'équations diophantiennes de degré supérieur.	**

1.61 Etude topologique d'ensembles de matrices de rang fixé

Référence : [Leb96]
Utilisation : (***,0) (**,1) (*,1)
Mots clefs : rang, calcul différentiel.

118	Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.	**
121	Déterminant. Applications.	*

1.62 Etude projective des quadriques

Référence : [Mne97]
Utilisation : (***,0) (**,2) (*,0)
Mots clefs : quadriques, espace projectif.

124	Formes quadratiques. Applications.	**
133	Exemples de propriétés projectives et d'utilisation d'éléments à l'infini.	**

1.63 Théorème de Cartan Von-Neumann

Référence : [MT97, p.64]
Utilisation : (***,0) (**,2) (*,0)
Mots clefs : racines de polynôme, coniques, inversion locale, exponentielle.

106	Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.	**
139	Exponentielle de matrices. Applications.	**

1.64 Classification des homographies de R^3

Référence : [Sid98]
Utilisation : (***,0) (**,2) (*,0)
Mots clefs : homographies, espaces projectifs, réduction des endomorphismes, sous-espaces stables.

122	Réduction d'un endomorphisme en dimension finie. Applications.	**
123	Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.	**

1.65 Etude des suites homographiques

Référence : [Vid01, p.59]
Utilisation : (***,0) (**,0) (*,1)
Mots clefs : homographies, itérations.

130	Homographies de la droite complexe. Applications.	*

1.66 Suites de Sturm

Référence : [Cia90, p.121][Gan66, p.10][Mig89, p.203]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : racines de polynômes, polynômes, algorithmes, localisation.

116	Racines des polynômes à une indéterminée. Relations entre les coefficients et les racines d'un polynôme. Exemples et applications.	**

1.67 Formule de Hadamard

Référence : [**?**]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : déterminant.

121	Déterminant. Applications.	**

1.68 Décomposition de Bruhat

Référence : [MT97]
Utilisation : (***,1) (**,0) (*,0)
Mots clefs : décomposition.

142	Exemples de décompositions remarquables dans le groupe linéaire. Applications.	***

1.69 Sous groupes algébriques de $GL(E)$, mesure de Haar et point fixe de Kakutani

Référence : [Ale99]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : point fixe, groupe linéaire.

106	Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.	**

1.70 Suite de Fibonacci et division euclidienne

Référence : [Dem97, p.25]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : suites récurrentes, complexité, algorithmes.

100	Méthodes combinatoires, problèmes de dénombrement. Séries génératrices.	**

1.71 Enveloppe convexe de $O(n)$

Référence : [ZQ95, p.201]
Utilisation : (***,0) (**,4) (*,0)
Mots clefs : séparation des convexes, enveloppe convexe, compacité, décomposition polaire.

125	Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie.	**
129	Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.	**
136	Formes linéaires sur un espace vectoriel de dimension finie. Espace dual, orthogonalité. Applications.	**
142	Exemples de décompositions remarquables dans le groupe linéaire. Applications.	**

1.72 Approximation diophantienne dans R^n

Référence : [Des86, p.48]
Utilisation : (***,0) (**,2) (*,0)
Mots clefs : réseau, théorème de Minkowski, formes linéaires.

102	Sous-groupes discrets de $\mathbb{R}^n$. Réseaux.	**
136	Formes linéaires sur un espace vectoriel de dimension finie. Espace dual, orthogonalité. Applications.	**

1.73 Théorème de Muntz

Référence : [Gou94b, p.286][Rud87, p.361]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : matrices, déterminant, projection, espaces denses.

121	Déterminant. Applications.	**

1.74 La fonction $\wp$ de Weierstrass

Référence : [Zis96, p.199]
Utilisation : (***,1) (**,0) (*,0)
Mots clefs : fonctions méromorphes, équation différentielle, série de fonctions.

102	Sous-groupes discrets de $\mathbb{R}^n$. Réseaux.	***

1.75 Forme quadratique de Lyapunov

Référence : [Arn74, p.199][GT96]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : forme quadratique, équations différentielles.

124	Formes quadratiques. Applications.	**

1.76 Lemme de Morse

Référence : [Gou94b, p.230]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : forme quadratique, calcul différentiel.

124	Formes quadratiques. Applications.	**

1.77 Le théorème des nombres premiers

Référence : [Tos99, p.1129]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : nombres premiers, transformée de Laplace, transformée de Fourier, fonction ζ, intégrales dépendant d'un paramètre, développement asymptotique.

109	Nombres premiers. Applications.	**

1.78 Méthodes de projection pour les équations intégrales

Référence : [Kre99, p.100]
Utilisation : (***,0) (**,0) (*,0)
Mots clefs : dimension finie, espaces complets, opérateurs compacts, méthodes de quadrature.

[pas de leçon l'utilisant]

1.79 Méthode de Nyström de résolution des équations intégrales

Référence : [Kre99, p.100]
Utilisation : (***,0) (**,1) (*,0)
Mots clefs : théorème d'Ascoli, équi-continuité, dimension finie, espaces complets, opérateurs compacts, méthodes de quadrature, approximation, projection.

135	Polynômes orthogonaux. Applications.	**

1.80 Polynômes orthogonaux et bases hilbertiennes

Référence : [?]
Utilisation : (***,1) (**,0) (*,0)
Mots clefs : polynômes orthogonaux, transformée de Fourier, fonctions holomorphes.

135	Polynômes orthogonaux. Applications.	***

2 Liste des leçons

2.101 Méthodes combinatoires, problèmes de dénombrement. Séries génératrices.

1 - Méthodes combinatoires classiques en algèbre et analyse:

. Séries génératrices et développements limités[FGS90] [*Application pour la détermination du nombre de relations d'équivalence*]

. Combinatoire des polyèdres[BY95, p.149]

. Croissance des groupes abéliens [*Citer les graphes de Cayley et la série génératrice associée*]

2 - Dénombrement et code correcteurs:

. Présentation des codes linéaires cycliques [*parler de la borne de Singleton*]

. Dénombrement, polynômes énumérateurs [*parler des codes parfaits*]

. Codes BCH, décodage [*parler de la distance apparente*]

3 - Actions de groupes:

. L'équation aux classes [*Applications pour les sous groupes finis de SO(3)*]

. Groupes simples[Per96] [*Utilisation des formules de Sylow*]

. Représentation linéaires des groupes finis

4 - Optimisation combinatoire:

. Présentation de la programmation linéaire

. CNS de minimum

. Algorithme du simplexe [*parler de l'initialisation*]

4	Représentation linéaire des groupes finis	***
23	Codes correcteurs linéaires cycliques [*polynômes énumérateurs, borne de Singleton, distance apparente des codes BCH*]	***

2.102 Groupe opérant sur un ensemble. Exemples et applications.

1 - Définition et premier exemples:

. Généralités [*stabilisateurs, orbites, équations aux classes*]

. Exemple de l'action de S_n sur un espace vectoriel [*théorème de Brauer*]

. Exemples d'actions géométriques [*les groupes finis de SO(3)*]

. Anneau des polynômes invariants, polynômes symétriques, application[CLO96, p.306]

2 - Autour de $PSL_2(\mathbb{Z})$:

. Présentation [*les homographies, le plan hyperbolique*]

. L'action sur le demi-plan de Poincarré [*génération du groupe, pavage et classification des réseaux*]

. Groupe d'automorphisme d'un code correcteur QR complété à l'infini [*utilisé la génération de PSL(2,Z)*]

3 - Représentation linéaire des groupes finis:

. Définitions [*représentations somme, irréductible, adjointe*]

. Représentation invariante, applications aux polynômes invariants[CLO96, p.306]

. Lemme de Schur, relation d'orthogonalité entre les caractères [*définir les caractères, le produit scalaire*]

. Représentation des groupes classiques [*groupe diédrale, groupe du carré*]

. Application au problème de la simplicité du groupe

4	Représentation linéaire des groupes finis [*faire un paragraphe sur les représentations linéaire, le lemme de Schur*]	***
5	Action du groupe modulaire sur le demi plan de Poincarré	***

2.103 Sous-groupes discrets de $\mathbb{R}^n$. Réseaux.

1 - Approximation diophantienne dans $\mathbb{R}^n$:

. Théorème de Minkowski et applications[Des86, p.49] [*application aux valeurs de fl sur Z*]

. Sous groupes discrets, denses, réseaux [*faire le théorème de décomposition d'un réseau*]

. Approximation diophantienne de formes linéaires

2 - Etude algébrique:

. $\mathbb{Z}$-modules et base adaptée[Art91, p.457] [*expliquer géométriquement le changement de base*]

. Classification des réseaux de $\mathbb{R}^2$ via l'action de $PSL_2(\mathbb{Z})$

3 - Applications à l'analyse et à l'algèbre:

. Fonction elliptique et fonction $\wp$ de Weierstrass. [*calculer les résidus sur un pavé*]

. Réseau d'un code correcteur [*présenter brièvement les codes cycliques*]

74	La fonction $\wp$ de Weierstrass	***
5	Action du groupe modulaire sur le demi plan de Poincarré [*insister sur la classification des réseaux*]	***

2.104 Sous-groupes distingués, groupes quotients. Exemples et applications.

1 - Définition et premiers exemples:

. Définitions[Per96, p.??]

. Exemples d'utilisation [*exemple de la récurrence de l'orthogonalité de caractères*]

2 - Le problème de la simplicité:

. Définition et quelques exemples

. Groupes de Sylow

. Etude de $PSL_n(K)$

3 - Le problème de la résolubilité:

. Définitions [*groupe dérivé, commutateur*]

. Etude de la résolubilité de A_n

. Application à la résolution d'équations par radicaux

4 - Applications des représentations linéaires:

. Définition d'une représentation

. Caractères, premières propriétés et lien avec les sous-groupes distingués

. Lecture des sous-groupes distingués sur la table des caractères

15	Transformée de Fourier sur un groupe fini [*utilisation d'un quotient pour faire une récurrence*]	***
4	Représentation linéaire des groupes finis [*application à l'étude de la simplicité du groupe*]	***

2.105 Groupes finis. Exemples et applications.

1 - Quelques exemples:

. Le cas simple : les groupes monogènes $\mathbb{Z}/p\mathbb{Z}$ [*donner des exemples de réalisation*]

. Le cas abélien : théorème de structure [*donner une application au groupe multiplicatif d'un corps fini, puis le théorème*

de Chevalley]

. Exemple de non commutativité : sous-groupes finis de $SO(3)$, groupe symétrique S_n

2 - Transformée de Fourier sur un groupe fini:

. Dual d'un groupe [*parler du bidual*]

. Relation d'orthogonalité, transformée de Fourier

. Approche via le théorème de structure [*expliquer le lien avec la transformée de Fourier multidimensionnelle*]

. Transformée de Fourier discrète, convolution

. Et dans le cas non commutatif? Le cas infini? Lien avec la transformée discrète, la transformée classique

3 - Représentation linéaire des groupes finis:

. Définitions [*représentations somme, irréductible, adjointe*]

. Lemme de Schur, relation d'orthogonalité entre les caractères [*définir les caractères, le produit scalaire*]

. Représentation des groupes classiques [*groupe diédrale, groupe du carré*]

. Application à l'étude de la simplicité du groupe

15	Transformée de Fourier sur un groupe fini	***
4	Représentation linéaire des groupes finis [*faire un paragraphe sur les représentations linéaire*]	***

2.106 Groupe des permutations d'un ensemble fini. Applications.

1 - Définitions, premières propriétés:

. Définitions [*décomposition en cycles, transpositions, signatures*]

. Polynômes symétriques [*décomposition en polynômes élémentaire, relation de Newton*]

. Résolubilité et application à la résolution par radicaux

2 - Autour de la représentation régulière:

. Définition d'une représentation linéaire [*donner l'action de S_n sur un ev*]

. Représentation par permutation, représentation régulière

. Théorème de Brauer [*donner les 4 preuves*]

. Caractères et relations d'orthogonalité [*dire qu'on a même une BON des fonctions centrales*]

. Décomposition de la représentation régulière

. Exemple du groupe du cube, S_4

3 - Applications:

. Formes de Hankel et nombres de racines réelles d'un polynôme [*expliquer qu'on utilise les relations de Newton*]

. Présentation des codes correcteurs cycliques

. Automorphismes d'un code QR complété [*action de $PSL(2,\mathbb{Z})$ par permutation*]

3	Théorème de Brauer	***
4	Représentation linéaire des groupes finis [*étude de S_4*]	***

2.107 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.

1 - Généralités:

. Définitions, sous-groupes importants[Per96, p.2]

. Etude de $PSL_n(K)$ [*simplicité, résolubilité*]

. Relation de similitude [*citer le théorème des invariants de similitudes*]

. Représentation régulière [*théorème de Brauer*]

2 - Etude topologique:

. Etude des sous groupes compacts [*donner le théorème, ses trois démonstrations, parler de mesure de Haar*]

. Exponentielle de matrice

. Sous groupes à 1 paramètre

. Etude des sous-groupes fermés [*théorème de Cartan-Von Neumann*]

3 - Représentation linéaire des groupes finis:

. Définitions [*représentations somme, irréductible, adjointe, théorème de Brauer*]

. Lemme de Schur, relation d'orthogonalité entre les caractères [*définir les caractères, le produit scalaire*]

. Représentation des groupes classiques [*groupe diédrale, groupe du carré*]

. Application à la simplicité

1	Sous groupes compacts de GL(E) [*faire un paragraphe sur les deux preuves*]	***
4	Représentation linéaire des groupes finis [*faire un paragraphe sur les représentations linéaire*]	***

2.108 Sous-groupes finis de $O(2,\mathbb{R})$, de $O(3,\mathbb{R})$. Applications.

1 - Etude de l'action de $O(2,\mathbb{R})$ et $O(3,\mathbb{R})$:

. Action de $O(2,\mathbb{R})$

. Les angles

. Action de $O(3,\mathbb{R})$

2 - Classification des sous groupes:

. Sous groupes de $O(2,\mathbb{R})$ [*groupes diédraux*]

. Sous groupes de $O(3,\mathbb{R})$

. Polyèdres et groupes polyédrique

3 - Représentation linéaire des groupes finis:

. Définitions [*représentations somme, irréductible, adjointe*]

. Lemme de Schur, relation d'orthogonalité entre les caractères [*définir les caractères, le produit scalaire*]

. Représentation des groupes classiques [*groupe diédrale, groupe du carré*]

24	Sous groupes finis de SO(3)	***
4	Représentation linéaire des groupes finis [*expliciter les représentations des groupes diédraux, etc.*]	***

2.109 Congruences dans $\mathbb{Z}/n\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.

1 - Généralités:

. $\mathbb{Z}/n\mathbb{Z}$, $\varphi(n)$, racines de l'unité

. Congruence dans $\mathbb{Z}$[Dem97, p.137]

. Structure des groupes abéliens finis[Art91, p.471]

. Cyclotomie modulo n

2 - Transformée de Fourier sur un groupe fini:

. Dual d'un groupe [*parler du bidual*]

. Relation d'orthogonalité, transformée de Fourier

. Approche via le théorème de structure [*expliquer le lien avec la transformée de Fourier multidimensionnelle*]

. La transformée de Fourier discrète, l'algorithme de la FFT [*citer des applications : multiplication de polynôme, simulation de fluides*]

. Application à la résolution de l'équation de Poisson par différences finies

3 - Codes correcteurs:

. Présentation des codes cycliques

. Codes BCH : présentation, décodage

. code QR : propriété, groupe d'automorphisme du code complété

15	Transformée de Fourier sur un groupe fini [*insister sur l'aspect Z-module*]	***
23	Codes correcteurs linéaires cycliques [*cyclotomie, décodage des codes BCH*]	***

2.110 Nombres premiers. Applications.

1 - Généralités, premières applications:

. Définition, premières propriétés[Dem97]

. Quelques tests de primalité [*insister sur l'utilisation des résidus quadratiques*]

. Application : crypto système RSA

2 - Corps finis et applications aux les codes correcteurs:

. Généralités sur les corps finis

. Factorisation de polynômes sur les corps finis [*algorithme de Berlekamp. Faire le parallèle factorisation sur les corps finis / dans* $\mathbb{Z}$]

. Présentation des codes cycliques

. Codes BCH : présentation, décodage

. code QR : propriété, groupe d'automorphisme du code complété

3 - Théorie analytique des nombres:

. La fonction ζ [*formule d'Euler, prolongement*]

. Un théorème taubérien [*expliquer la formulation en terme de séries de Dirichlet*]

. Le théorème sur les nombres premiers

21	Algorithme de Berlekamp	***
23	Codes correcteurs linéaires cycliques [*cyclotomie, décodage des codes BCH*]	***

2.111 Idéaux d'un anneau commutatif unitaire. Exemples et applications.

1 - Généralité et mise en situation:

. Définition et premiers exemples [*idéaux principaux, quotientage, théorème de correspondance, idéaux premiers/maximaux*]

. Idéaux et arithmétique [*PGCD, PPCM*]

. Idéaux et variétés algébriques [*notation, théorème de la base de Hilbert*]

. Polynômes invariants et idéal des relations

2 - Anneaux de polynômes, application aux bases de Gröbner:

. Algorithme de division

. Idéaux de monômes

. Théorème de la base de Hilbert

. Bases de Gröbner

. Applications à l'élimination

3 - Courbes algébriques:

. Idéaux et variétés

. Théorème des zéros

. Courbes algébriques rationnelles

4 - Codes correcteurs cycliques:

. Présentation des codes cycliques

. Cyclotomie modulo n

. Codes BCH : présentation et décodage

22	Bases de Gröbner	***
23	Codes correcteurs linéaires cycliques [*idéal d'un code cyclique, décodage des BCH*]	***
41	Théorème des zéros de Hilbert	***

2.112 Corps finis. Applications.

1 - Généralités:

. Structure des corps finis[Dem97, p.195] [*corps premier, structure, automorphisme, construction*]

. Groupe multiplicatif, théorème de Chevalley [*utilisation du théorème de structure de groups abélien finis*]

2 - Polynômes sur un corps fini:

. Le théorème de Chevalley

. Cyclotomie sur un corps fini

. Algorithme de Berlekamp

3 - Les codes correcteurs:

. Présentation des codes cycliques

. Codes BCH : présentation et décodage

. Codes QR

21	Algorithme de Berlekamp	***
23	Codes correcteurs linéaires cycliques [*cyclotomie, décodage des BCH*]	***

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

1 - Généralités:

. Définitions [*corps de fractions, degré, dérivation, représentation irréductible*]

. Décomposition en éléments simples

. Applications [*Gauss-Lucas, relations de Newton, calcul de dérivées et primitives*]

2 - Paramétrisation rationnelle de courbes:

. Courbes rationnelles [*définition, intersection de courbes planes, paramétrisation des coniques*]

. Utilisation du résultant

. Courbes de Bezier et NURBS

3 - Un peu d'analyse:

. Homographies

. Transformation de Joukowsky et fluides incompressibles

. Interpolation rationnelle

27	Courbes rationnelles	***
41	Théorème des zéros de Hilbert	***

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

1 - Généralités, premiers exemples:

. Irréductibilité [*définition, irréductibilité sur $Frac(A)$, contenu, lemme de Gauss*]

. Critères [*Eisenstein, réduction, critère dans $\mathbb{R}$*]

. Corps de rupture, de décomposition

. Applications en théorie de Galois[Goz97]

. Application aux nombres constructibles

2 - Polynômes sur un corps fini:

. Définition des corps finis [*corps de décomposition de $X^q - X$*]

. Algorithme de Berlekamp

. Polynômes irréductibles sur un corps fini[Dem97, p.207] [*décomposition, dénombrement*]

. Cyclotomie sur un corps finis

3 - Les codes correcteurs:

. Présentation des codes cycliques

. Codes BCH : présentation et décodage

. Codes QR

21	Algorithme de Berlekamp	***
23	Codes correcteurs linéaires cycliques [*corps cyclotomiques, décodage des BCH*]	***

2.115 Groupe des nombres complexes de module 1. Applications.

1 - Généralités:

. Racines de l'unités, définition de π[Rud87]

. Exponentielle complexe[Rud87]

. Angle, mesure d'un angle[Aud98]

. Sous groupes de $SO(2)$

. Autour du cercle $\{|z| = 1\}$ [*paramétrisation rationnelle, triplets pythagoriciens*]

2 - Cyclotomie:

. Polynômes cyclotomiques [*définition, application au théorème de Wederburn*]

. Cyclotomie modulo n

. Application aux codes correcteurs [*codes BCH*]

3 - Transformée de Fourier sur un groupe abélien fini:

. Définition du dual d'un groupe

. Quelques groupes infinis [*cas du tore et de la droite*]

. Le cas des groupes finis

. Etude à l'aide du théorème de structure

. Quelques mots sur les représentations [*recherche de sous groupes distingués*]

4 - Application au traitement du signal:

. Transformée de Fourier discrète

. Algorithme FFT

. Applications [*convolutions, multiplications de polynômes, résolution de l'équation de la chaleur, calcul de coefficients de Fourier*]

15	Transformée de Fourier sur un groupe fini [*étude algébrique*]	***
16	Transformée de Fourier discrète [*utilisation de la FFT, application à l'équation de Poisson*]	***

2.116 Algèbre des polynômes à n indéterminées ($n \geq 2$). Polynômes symétriques. Applications.

1 - Généralités:

. Structure des algèbres de polynômes [*théorème de la base de Hilbert, factorialité*]

. Polynômes symétriques, sommes de Newton

. Polynômes invariants[CLO96, p.306] [*idéal des relations, opérateur de Reynolds*]

. Applications : formes de Hankel et nombre de racines réelles

2 - Ensembles algébriques:

. Définitions et notations

. Quelques exemples

. Courbes rationnelles

3 - Résultant et élimination:

. Résultant de Sylvester, formulation de Bezout

. Exemples d'applications [*intersection de surfaces, calcul d'équations implicites, nombres algébriques*]

. Introduction au résultant en plusieurs variables

4 - Bases de Gröbner:

. Ordre sur les monômes, algorithme de division [*expliquer les problème du reste*]

. Bases de Gröbner : définition et premières propriétés

. Algorithme de calcul [*expliquer les propriétés du poynôme-S*]

. Quelques applications [*coloriage de graphes et cinématique inverse*]

41	Théorème des zéros de Hilbert	***
22	Bases de Gröbner	***
27	Courbes rationnelles	***

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

1 - Généralités:

. Structure de $K[X]$, relation coefficients racines, sommes de Newton [*application au théorème de Cayley-Hamilton*]

. Application : formes de Hankel, nombre de racines réelles

. Les cas simple des corps finis [*algorithme de Berlekamp*]

2 - Problème de localisation:

. Localisation grossière[Mig89, p.154]

. Suites de Sturm

. Un algorithme efficace : méthode de Laguerre

. Application : recherche des zéros des polynômes orthogonaux, application aux méthodes de gauss

. Un problème classique : stabilité des systèmes dynamiques [*critère de Routh*]

. Recherche de zéros communs : résultant et discriminant [*expliquer le lien avec le PGCD*]

3 - Théorie des corps, cyclotomie. Application aux codes correcteurs:

. Corps de rupture et de décomposition

. Cyclotomie modulo p

. Présentation des codes cycliques

. Codes BCH : présentation et décodage [*utilisation des relations coefficients racines et division euclidienne*]

23	Codes correcteurs linéaires cycliques [*racines primitives, diviseurs cyclotomiques, code BCH (expliquer l'utilisation des relation C/R)*]	***
21	Algorithme de Berlekamp [*faire un paragraphe sur les corps finis*]	***

2.118 Équations diophantiennes du premier degré $ax + by = c$. Exemples d'équations diophantiennes de degré supérieur.

1 - PGCD, PPCM et équations diophantiennes du 1er degrés:

. Algorithme de calcul du PGCD, complexité[Dem97, p.19]

. Interprétation dans le cadre des anneaux euclidiens et factoriels

. Application aux équations diophantiennes

2 - Courbes et équations diophantiennes:

. Courbes rationnelles, définitions

. Paramétrisation rationnelle des coniques

. Triplet pythagoriciens

. Sur les corps finis : théorème de Chevalley

3 - Approximations diophantiennes:

. Approximations diophantiennes et fractions continues

. Application aux sommes de deux carrés

. Application à l'équation de Pell

4 - Application aux codes correcteurs:

. Présentation des codes cycliques

. Cyclotomie modulo p

. Codes BCH : présentation et décodage

27	Courbes rationnelles [*insister sur les triplets pythagoriciens*]	***
28	Corps finis et théorème de Chevalley	***

2.119 Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

1 - Généralités, premières applications:

. Définitions [*rang, déterminant extrait*]

. Application : détermination du nombre de racines réelles [*formes de Hankel*]

. Algorithme de Berlekamp

2 - Codes correcteurs:

. Présentation des codes cycliques

. Cyclotomie modulo p

. Codes BCH : présentation et décodage

3 - Programmation linéaire:

. Présentation de la programmation linéaire

. CNS de minimum

. Algorithme du simplexe [*parler de l'initialisation*]

4 - Représentation linéaire des groupes finis:

. Définitions [*représentations somme, irréductible, adjointe*]

. Lemme de Schur, relation d'orthogonalité entre les caractères [*définir les caractères, le produit scalaire*]

. Représentation des groupes classiques [*groupe diédrale, groupe du carré*]

21	Algorithme de Berlekamp [*insister sur l'utilisation du rang*]	***
4	Représentation linéaire des groupes finis [*faire un paragraphe sur les représentations linéaire*]	***

2.120 Matrices équivalentes. Matrices semblables. Applications.

1 - Définition, réduction, premiers exemples:

. Généralités [*relation de similitude, changement de base, réduction selon le rang*]

. Action de S_n sur un espace vectoriel [*théorème de Brauer*]

. Trigonalisation, diagonalisation[RDO79, p.294]

. Diagonalisation des endomorphismes symétriques, applications [*lignes de courbures, axes des coniques, matrice d'inertie*]

. Une vision géométrique : quadriques et classes de similitude

2 - Invariants de similitudes:

. Approche algébriques, dualité [*expliquer en quoi ça résout le problème de similitude*]

. Modules de type fini sur un anneau euclidien[Art91, p.451] [*réduction de matrice, base adaptée, invariants*]

. Applications aux réseaux et aux générateurs/relations

. Algorithme de calcul des invariants de similitude

. Application aux systèmes différentiels linéaires [*réduction de Jordan et calcul de l'exponentielle*]

3 - Décompositions matricielles et applications:

. Méthode de Gauss, décomposition LU et de Cholesky

. Décomposition QR [*expliquer les matrices de Householder*]

. Méthode QR et recherche de valeurs propres

4 - Représentation linéaire des groupes finis:

. Définitions [*représentations somme, irréductible, adjointe*]

. Représentation par permutation, représentation régulière [*application au théorème de Brauer*]

. Lemme de Schur, relation d'orthogonalité entre les caractères [*définir les caractères, le produit scalaire*]

. Représentation des groupes classiques [*groupe diédrale, groupe du carré*]

3	Théorème de Brauer	***
4	Représentation linéaire des groupes finis [*parler de représentations équivalentes*]	***
14	Quadriques et classes de similitudes	***
8	Invariants de similitude, version algébrique	***

2.121 Opérations élémentaires sur les lignes et les colonnes d'une matrice. Résolution d'un système d'équations linéaires. Applications.

1 - Généralités:

. Opérations élémentaires sur un anneau euclidien[Gob95a] [*matrices associées*]

. Application à l'étude de $PSL_n(K)$[Per96] [*étude de la simplicité*]

2 - Autour des invariants de similitude:

. Modules de type fini sur un anneau euclidien[Art91, p.451] [*réduction de matrice, base adaptée, invariants*]

. Applications aux réseaux et aux générateurs/relations
. Algorithme de calcul des invariants de similitude [*expliquer la relation entre $K[X]$-modules et applications linéaires*]
. Application aux systèmes différentiels linéaires [*réduction de Jordan et calcul de l'exponentielle*]

3 - Algorithmes numériques:

. Méthode de Gauss, décomposition LUA et de Cholesky[Cia90, p.71]
. Décomposition QR [*expliquer les matrices de Householder*]
. Méthode QR et recherche de valeurs propres

9	Invariants de similitude, version euclidienne	***
45	Simplicité de $PSL_n(Z)$	***

2.122 Déterminant. Applications.

1 - Généralités:

. Définitions [*mineurs principaux*]
. Méthodes de Kramer [*c'est un outil théorique*]
. Application : ensemble de matrices de rang fixé

2 - Outils théoriques:

. Polynôme caractéristique, réduction d'endomorphisme
. Optimisation du déterminant [*sous groupes compacts (ellipsoïdes de John), base d'Auerbach*]
. Calcul de projections [*matrices de Gram, théorème de Muntz*]

3 - Outil calculatoire : le résultant:

. Résultant de Sylvester, propriétés, utilisation dans le cas de plusieurs variables
. Théorie de l'élimination [*théorème d'extension, interprétation géométrique*]
. Exemples d'applications [*intersection de surfaces, calcul d'équations implicites, nombres algébriques*]
. Résolution de systèmes polynomiaux [*exemple de la cinématique inverse*]

2	Sous groupes compacts de GL(E), utilisation des ellipsoïdes de volume minimal [*insister sur le raport volume/déterminant*]	***
27	Courbes rationnelles [*utilisation du résultant pour l'intersection de courbes planes, théorème d'extension*]	***

2.123 Réduction d'un endomorphisme en dimension finie. Applications.

1 - Diagonalisation, trigonalisation:

. Définitions[RDO79, p.394] [*espaces propres, polynôme caractéristique, polynôme minimal*]
. Trigonalisation, diagonalisation
. Espaces caractéristiques, décomposition de Dunford, de Jordan

2 - Applications:

. Topologie de $M_n(\mathbb{C})$[MT97, p.14] [*densité de $GL_n(\mathbb{C})$, $\chi_{AB} = \chi_{BA}$*]
. Théorème de Brauer [*dans ce cas, on a une réponse simple au problème*]
. Calcul des puissance d'une matrice [*suites récurrentes*]
. Calcul de l'exponentielle d'une matrice, résolution de système différentiels linéaires[Art91, p.481]

3 - Autour des invariants de similitude:

. Etude algébrique
. $K[X]$-modules, approche algorithmique
. Application au problème de similitude

4 - Représentations linéaires:

. Représentations irréductibles

. Caractères [*insister sur le fait que les matrices de représentation sont diagonalisables*]

. Application à la simplicité

8	Invariants de similitude, version algébrique	***
4	Représentation linéaire des groupes finis [*parler de représentations équivalentes, la simplicité*]	***

2.124 Sous-espaces stables d'un endomorphisme d'un espace vectoriel de dimension finie. Applications.

1 - Réduction des endomorphismes:

. Sous espaces propres, trigonalisation, diagonalisation

. Sous espaces caractéristiques, réduction de Dunford, de Jordan [*application aux systèmes différentiels linéaires*]

. Le langage des $K[X]$-modules, les invariants de similitude [*expliquer la traduction des sous modules*]

2 - Représentation linéaire des groupes finis:

. Définitions [*insister sur l'irréductibilité, la somme de représentations*]

. Lemme de Schur, relation d'orthogonalité entre les caractères [*définir les caractères, le produit scalaire*]

. Représentation des groupes classiques [*groupe diédrale, groupe du carré*]

. Application à la simplicité

3 - Codes correcteurs cycliques:

. Présentation des codes cycliques [*expliquer que l'on retrouve la notion de stabilité, d'idéaux*]

. Automorphismes d'un code [*les codes sont les sous-espaces stables des endomorphismes*]

. Automorphismes des codes QR complétés

8	Invariants de similitude, version algébrique	***
4	Représentation linéaire des groupes finis [*parler de représentations irréductibles*]	***

2.125 Formes quadratiques. Applications.

1 - Généralités:

. Définitions [*formes quadratique, orthogonalité, dégénérescence*]

. Bases orthogonales, orthogonalisation [*présenter le résultat d'orthogonalisation simultanée*]

. Classification des formes quadratiques [*sur R, C et les corps finis*]

2 - Coniques et quadriques:

. Définition, quadriques projective, classification

. Le mouvement des planètes

. Quadriques comme sous ensembles matriciels

3 - Applications:

. Calcul différentiel [*CNS d'extremum, lemme de Morse, direction de courbures*]

. Cinématique du solide [*énergie cinétique, axe d'inertie*]

. Nombre de racines d'un polynôme [*formes de Hankel*]

13	Formes de Hankel et nombres de racines d'un polynôme	***
14	Quadriques et classes de similitudes	***

2.126 Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie.

1 - Généralités:

. Le groupe orthogonal[Per96][Aud98] [*étudier la génération, la simplicité de* $PSO(n)$]

. Endomorphismes symétriques[RDO79, p.36] [*adjoints, diagonalisation, réduction simultanée*]

2 - Etude topologique des sous groupes de $GL_n(\mathbb{R})$:

. Décomposition polaires et applications[MT97, p.18] [*enveloppe convexe de O(n), homéomorphisme*]

. Exponentielle [*homéomorphisme résultant*]

. Les sous groupes compacts : étude géométrique [*construction de point fixe*]

. Ellipsoïde de John

3 - Les rotations de l'espace de dimension 3:

. Les quaternions [*expliquer l'utilisation de PSU(2)*]

. Rotation et homographies [*expliquer la projection stéréographique, les homographies isométriques*]

. Etude de l'isomorphisme $SO(3) \simeq PSU(2)$ [*introduire l'exponentielle*]

1	Sous groupes compacts de GL(E)	***
10	Etude topologique de SO(3) via les quaternions	***

2.127 Endomorphismes remarquables d'un espace vectoriel hermitien de dimension finie.

1 - Généralités:

. Le groupe unitaire

. Endomorphismes auto-adjoints, endomorphismes unitaires, normaux

. Décomposition polaires et applications

2 - Les rotations de l'espace de dimension 3:

. L'exponentielle de matrice [*exponentielle d'une matrice anti-symétrique, lien avec les rotations*]

. Les quaternions [*expliquer l'utilisation de PSU(2)*]

. Rotation et homographies [*expliquer la projection stéréographique, les homographies isométriques*]

. Etude de l'isomorphisme $SO(3) \simeq PSU(2)$ [*introduire l'exponentielle*]

3 - Transformée de Fourier sur un groupe fini:

. Espace hermitien des fonctions de G dans $\mathbb{C}$

. Caractères, transformée de Fourier

. Le cas non commutatif, représentation linéaire de groupe [*intervention de* $\mathbb{C}$ *dans le lemme de Schur, représentations unitaires*]

10	Etude topologique de SO(3) via les quaternions	***
4	Représentation linéaire des groupes finis [*insister sur les représentation unitaires, et sur le fait qu'on a un produit scalaire hermitien*]	***

2.128 Isométries d'un espace affine euclidien de dimension finie. Formes réduites. Applications.

1 - Généralités:

. Définitions[Aud98, p.15] [*applications affines, décomposition*]

. Propriétés, décomposition d'une isométrie

. Exemples [*symétries, translations*]
. Barycentre [*expliquer l'espace universel*]
. Structures des isométries, déplacements [*décomposition en produit de réflexions*]

2 - Géométrie plane:

. Angles orientés
. Classification des isométries planes
. Similitudes
. Inversions, groupe circulaire [*conservation des droites et des cercles*]

3 - Applications:

. Groupes de pavages
. Champs équiprojectifs [*expliquer les utilisations en physique*]

11	Champs équiprojectifs, application à la cinématique	***
32	Forme réduite d'une application affine	***

2.129 Coniques.

1 - Généralités:

. Définition bifocale et équations[Aud98, p.179]
. Coniques et angles [*propriétés optiques, théorème de l'angle pivotant*]

2 - Coniques projectives:

. Coniques propre, homogénéisée[Aud98, p.185]
. Classification

3 - Applications:

. Mouvement des planètes
. Coniques et racines de polynômes [*petit théorème de Poncelet*]
. Paramétrisation rationnelle, courbes de bézier rationnelles

20	Théorème de l'angle pivotant	***
25	2ème théorème de Poncelet	***

2.130 Barycentres dans un espace affine réel de dimension finie ; convexité. Applications.

1 - Généralités:

. Barycentres[Gob95a, p.35] [*parler de l'espace universel*]
. Utilisation : sous-groupes compacts de $GL_n(\mathbb{R})$
. Barycentres et régionnement
. Convexité, enveloppe convexe, points extrémaux [*donner l'exemple de l'enveloppe convexe de O(n)*]

2 - Polyèdres:

. Définitions et premières propriétés [*demi-espaces, facettes*]
. Combinatoire[BY95, p.149]
. Dualité
. Algorithmes [*recherche d'enveloppes convexes*]

3 - Programmation linéaire et programmation convexe:

. Programmation convexe et relation de Kuhn et Tucker[Cia90, p.202] [*insister sur le lemme de Farkas-Minkowski*]

. Problèmes de programmation linéaire [*donner un exemple*]
. Existence de solution en programmation linéaire

1	Sous groupes compacts de GL(E)	***
12	Existence de solution en programmation linéaire	***

2.131 Homographies de la droite complexe. Applications.

1 - Généralités:
. Droite projective
. Homographies[Aud98] [*définition, birapport*]
. Application : suites homographiques
2 - Propriétés des homographies:
. Groupe circulaire, conservation des droites et des cercles
. Transformation conformes de $\mathbb{P}^1(\mathbb{C})$
. Isométries du plan hyperbolique
3 - Utilisation des homographies:
. Action de $PSL_2(\mathbb{Z})$ sur le demi-plan de Poincarré [*insister sur les applications*]
. Etude de $SO(3)$ via les quaternions, via les homographies [*expliquer la projection stéréographique*]
. Automorphisme d'un code QR complété

5	Action du groupe modulaire sur le demi plan de Poincarré	***
7	Applications conformes de la droite projective complexe	***

2.132 Applications des nombres complexes à la géométrie.

1 - Les plan complexe, la droite projective:
. Nombre complexes et isométries
. Nombres complexes et constructions à la règle et au compas
. La droite projective et les homographies [*expliquer la projection stéréographique*]
2 - Propriétés géométriques des homographies:
. Conservation des droites et des cercles
. Transformation conformes de $\mathbb{P}^1(\mathbb{C})$
. Isométries du plan hyperbolique
3 - Utilisation des homographies et des transformations holomorphes:
. Action de $PSL_2(\mathbb{Z})$ sur le demi-plan de Poincarré [*insister sur les applications géométriques*]
. Etude de $SO(3)$ via les quaternions, via les homographies
. Fluides incompressibles [*transformation* $\frac{1}{2}(z + 1/z)$]

5	Action du groupe modulaire sur le demi plan de Poincarré	***
10	Etude topologique de SO(3) via les quaternions	***

2.133 Utilisation des angles en géométrie.

1 - Généralités:
. Notion d'angle en dimension 2 [*groupe du cercle, SO(2)*]

. En dimension supérieure
. Un exemple historique : la trisection d'un angle[Car89]

2 - Angles et coniques:
. Définition par cercles des coniques
. Propriétés "optiques" des coniques [*théorème de l'angle pivotant*]
. Généralisation : caustique d'une courbe [*exemple de la caustique d'un cercle, résolution avec le résultant*]
. Coniques et racines de polynômes [*2e théorème de Poncelet*]

3 - Applications conformes:
. Droite projective et homographies
. Applications conformes de $\mathbb{P}^1(\mathbb{C})$
. Application aux fluides incompressibles et irrotationnels

20	Théorème de l'angle pivotant	***
7	Applications conformes de la droite projective complexe	***

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

1 - Généralités:
. Espaces projectifs
. Dualité [*faire une liste de propriétés duales, et les théorèmes de Papus et Desargues*]
. Quadriques projectives[Aud98, p.185] [*notion de quadrique propres, classification en dimension 2 et 3*]

2 - Droite projective et homographies:
. Définition
. Conservation des droites et des cercles
. Transformation conformes de $\mathbb{P}^1(\mathbb{C})$

3 - Applications:
. Etude topologique de $SO(3)$
. Code correcteur QR complété à l'infini
. Fluides incompressible [*utilisation de singularité en l'infini*]

6	Etude du groupe circulaire	***
7	Applications conformes de la droite projective complexe	***

2.135 Constructions à la règle et au compas.

1 - Quelques figures élémentaires:
. Dans le triangle
. Construction élémentaires [*à utiliser pour la construction du corps des nombres constructibles*]
. Courbes de Bezier : algorithme de subdivision

2 - Coniques et angles:
. Définition bifocales des coniques
. Définition avec cercles des coniques
. Propriétés "optiques" des coniques [*théorème de l'angle pivotant*]
. Dualité pour une conique

3 - Etude algébrique:
. Extension de corps [*corps de rupture, extension*]

. Nombre constructibles à la règle et au compas
. Polygones constructibles
. La construction au compas seulement

26	Nombres constructibles à la règle et au compas	***
20	Théorème de l'angle pivotant [*insister sur la caractérisation de la tangence*]	***

2.136 Polynômes orthogonaux. Applications.

1 - Généralités:
. Définitions
. Propriétés
. Exemples classiques
. Bases hilbertiennes de polynômes orthogonaux
2 - Méthodes de quadrature numérique:
. Définition, exemples [*méthodes de Newton-Cotes*]
. Formule de l'erreur, problème de choix des points d'interpolation
. Méthode de Gauss [*donner les exemples classiques, expliquer les avantages*]
3 - Application aux équations intégrales:
. Position du problème
. Méthode Nyström [*écrire le système linéaire résultant*]
. Equation du transport lumineux : problème de singularité [*mettre en avant l'utilisation de méthodes intégrant la singularité*]

31	Polynômes orthogonaux	***
80	Polynômes orthogonaux et bases hilbertiennes	***

2.137 Formes linéaires sur un espace vectoriel de dimension finie. Espace dual, orthogonalité. Applications.

1 - Généralité:
. Définition [*dualité, crochet, base duale, bidual*]
. Dualité et orthogonalité [*matrice adjointe, sous espaces stables*]
. Dualité projective [*théorèmes de Desargues, Papus*]
2 - Approche géométrique:
. Séparation des compacts [*Application : enveloppe convexe de O(n)*]
. Dualité entre les polyèdres [*dualité vecteurs/hyperplans*]
. Dualité pour une quadrique
. Programmation linéaire [*expliquer le lemme de Farkas, ainsi que l'idée de l'algorithme du simplexe*]
3 - Applications:
. Codes linéaires [*décodage par syndrome*]
. Interpolation Lagrange
. Représentations linéaires [*représentations duales et des morphismes*]

8	Invariants de similitude, version algébrique	***
4	Représentation linéaire des groupes finis	***
12	Existence de solution en programmation linéaire	***

2.138 Exemples de parties génératrices d'un groupe.

1 - Généralités:

. Définitions [*groupes cycliques, groupes monogènes, groupes finis*]

. Modules sur un anneau euclidien, bases adaptées, applications aux réseaux

. Structure des groupes abéliens

. Application à la transformée de Fourier [*expliquer le rapport avec la TFD multidimensionnelle*]

2 - Quelques exemples classiques:

. Groupe symétrique [*génération, simplicité*]

. Groupe linéaire [*transvections, simplicité de* $PSL_n(K)$]

. Les isométries[Aud98]

3 - Autour du groupe modulaire:

. Action sur le demi plan de Poincarré

. Génération

. Application aux codes correcteurs QR

4 - Etude de croissance de groupes:

. Types de croissance

. Exemples [*pour* $PSL_n(\mathbb{Z})$*, expliquer l'utilisation de la génération par* (S,T)]

. Métrique associées, graphes de Cayley

5	Action du groupe modulaire sur le demi plan de Poincarré [*insister sur les applications (codes QR, réseaux, pavage)*]	***
15	Transformée de Fourier sur un groupe fini [*utilisation le théorème de structure*]	***

2.139 Endomorphismes diagonalisables.

1 - Réduction d'endomorphismes:

. Espaces propres, polynômes caractéristique

. Trigonalisation, diagonalisation

. Espaces caractéristiques, décomposition de Dunford

. Endomorphismes symétriques

2 - Invariants de similitude, étude algébrique:

. Preuve par dualité

. Application au problème de similitude

. Décomposition de Jordan

. Application aux systèmes différentiels linéaires[Art91]

3 - Invariants de similitude, version euclidienne:

. Diagonalisation des matrices sur un anneau euclidien

. Applications aux réseaux et aux générateurs/relations

. Langage des $K[X]$-modules, liens avec les invariants de similitude

. Algorithme de calcul des invariants

4 - Représentations linaires:

. Définitions

. Caractères, sous-groupes distingués

. Utilisation de la table des caractères

8	Invariants de similitude, version algébrique	***
4	Représentation linéaire des groupes finis [*application à la simplicité du groupe*]	***

2.140 Exponentielle de matrices. Applications.

1 - Généralités:

. Définition

. Propriétés

. Fonctions matricielles

2 - Etude des systèmes différentiels linéaires:

. Systèmes à coefficients constants

. Le cas général

. Réduction de Jordan et application au calcul de l'exponentielle[Art91, p.381]

. Sous groupes à paramètres

3 - Etude topologique:

. Homéomorphismes résultants

. Quaternions et étude de $SO(3)$ [*expliqué l'isomorphisme inverse fourni par l'exponentielle*]

. Etude des sous groupes de $GL_n(\mathbb{R})$ [*théorème de Cartan-Von Neumann, pas de sous-groupes de taille petite*]

10	Etude topologique de SO(3) via les quaternions	***
29	Groupes à paramètres d'automorphismes	***

2.141 Endomorphismes nilpotents.

1 - Réduction matricielle:

. Définitions [*espaces propres, polynôme caractéristique, minimal*]

. Sous-espaces caractéristiques, décomposition de Dunford

. Décomposition de Jordan

2 - Exponentielle de matrice:

. Calcul explicite[Art91, p.381]

. Résolution de systèmes différentiels linéaires

. Inversion de l'exponentielle

3 - Orbites de nilpotence:

. Définition[Mne97]

. Tableau de Young

18	Décomposition de Jordan et applications	***
36	Etude de l'exponentielle de matrice [*homéomorphisme des nilpotent sur les idempotent*]	***

2.142 Polynômes d'endomorphismes. Applications.

1 - Réductions des endomorphismes:

. Polynôme caractéristique [*espace propres, valeurs propres*]

. Polynôme minimal, diagonalisation

. Espaces caractéristiques, décomposition de Dunford

. Application : le théorème de Brauer

2 - Les invariants de similitude:

. Approche algébrique

. Théorème de structure, approche algorithmique des invariants

. Application au problème de similitude

3 - Exponentielle de matrices:

. Définition, premières propriétés

. Fonctions matricielles

. Réduction de Jordan : calcul effectif

. Application : résolution de systèmes linaires

. Application : étude de $SO(3)$

3	Théorème de Brauer	***
8	Invariants de similitude, version algébrique	***

2.143 Exemples de décompositions remarquables dans le groupe linéaire. Applications.

1 - Transvections et groupe spécial linéaire:

. Définitions[Per96] [*les transvections, PSL(2,K)*]

. Génération de $PSL(2,K)$

. Simplicité, résolubilité

2 - Décomposition polaire et de Bruhat:

. La décomposition polaire[MT97] [*homéomorphisme résultant*]

. Applications [*enveloppe convexe de O(n)*]

. La décomposition de Bruhat

3 - Algorithmes numériques:

. Méthode de Gauss, décomposition LUA et de Cholesky[Cia90]

. Décomposition QR [*expliquer les matrices de Householder*]

. Méthode QR et recherche de valeurs propres

17	Factorisation QR et méthode QR de recherche de valeurs propres	***
68	Décomposition de Bruhat	***

2.144 Problèmes d'angles et de distances.

1 - Généralités:

. Définitions [*isométries, angles en dimension 2 et plus*]

. Figures élémentaires [*propriétés du triangles*]

. Nombres constructibles à la règle et au compas [*quadrature du cercle et trisection d'un angle*]

2 - Coniques et angles:

. Définition par foyer/directrice

. Définitions par cercles

. Propriétés "optiques" des coniques [*théorème de l'angle pivotant, de Poncelet*]

. Dualité pour une conique

3 - Application conforme:

. Définition
. Application conforme de $\mathbb{P}^1(\mathbb{C})$, lien avec le groupe de Moébius
. Utilisation pour les fluides incompressibles et irrotationnels

7	Applications conformes de la droite projective complexe	***
20	Théorème de l'angle pivotant	***

2.145 Utilisation des groupes en géométrie.

1 - Généralités, actions de groupes:
. Définitions, premiers exemples
. Géométries vectorielle et affine
. Groupes de pavages
2 - Autour des isométries:
. Isométries et angles
. Isométries et polyèdres
. Rotations et quaternions
3 - Représentation linéaire des groupes finis:
. Définitions [*représentations somme, irréductible, adjointe*]
. Lemme de Schur, relation d'orthogonalité entre les caractères [*définir les caractères, le produit scalaire*]
. Etude de quelques groupes géométriques classiques [*groupe diédrale, groupe du carré*]
4 - Autour du groupe modulaire:
. La droite projective et les homographies [*conservation des droites et des cercles*]
. Application conformes de $\mathbb{P}^1(\mathbb{C})$
. Action de $PSL_2(\mathbb{Z})$ sur le demi plan de Poincarré [*expliquer les applications*]

1	Sous groupes compacts de GL(E)	***
5	Action du groupe modulaire sur le demi plan de Poincarré	***

Références

[AB93] Arnaudies and Bertin. *Groupes, algèbres, et géométrie, Tome 1.* Ellipses, 1993.

[Ale99] Alessandri. *Thèmes de géométrie.* Masson, 1999.

[Arn74] V Arnold. *Equations différentielles ordinaires.* Librairie du globe, 1974.

[Arn76] V Arnold. *Méthodes mathématiques de la mécanique classique.* MIR, 1976.

[Art91] Michael Artin. *Algebra.* Prentice Hall, 1991.

[Aud98] Michèle Audin. *Géométrie pour l'agrégation.* Belin, 1998.

[BR74] Alain Bouvier and Denis Richard. *Groupes. Observation, théorie, pratique.* Herman, 1974.

[BY95] Jean-Daniel Boissonnat and Mariette Yvinec. *Géométrie algorithmique.* Ediscience international, 1995.

[Car61] Cartan. *Théorie élémentaire des fonctions d'une variable complexe.* Herman, 1961.

[Car89] Jean Claude Carrega. *Théorie des corps. La règle et le compas.* Herman, 1989.

[Car97] Cartan. *Calcul différentiel.* Herman, 1997.

[Cia90] Philippe G. Ciarlet. *Introduction à lanalyse numérique et à l'optimisation.* Dunod, 1990.

[CLO96] D. Cox, J. Little, and O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Algebraic Geometry and Commutative Algebra, 2nd ed.* Springer-Verlag, 1996.

[CLR92] Thomas Cormen, Charles Leiserson, and Ronald Rivest. *Introduction à l'algorithmique.* Dunod, 1992.

[CS97] David A. Cox and Bernd Sturmfels. *Applications of computational algebraic geometry.* American Mathematical Society, 1997.

[Dem96] Jean Pierre Demailly. *Analyse numérique et équations différentielles.* EDP, 1996.

[Dem97] Michel Demazure. *Cours d'algèbre. Primalité, divisibilité, codes.* Cassini, 1997.

[Des86] Roger Descombes. *Elements de théorie des nombres.* PUF, 1986.

[DMK72] H. Dym and HP. Mc Keam. *Fourier series and integrals.* Academic press, 1972.

[Dub53] Dubreil. *Leçons sur la théorie des treillis des structures algébriques ordonnées et des treillis géométriques.* Gauthier-Villars, 1953.

[Fer01] Ferrand. *Polycopié de M.Ferrand.* Université de Rennes 1, 2001.

[FGS90] Christine Froidevaux, Marie-Claude Gaudel, and Michèle Soria. *Types de données et algorithmes.* Ediscience international, 1990.

[Gan66] F.R. Gantmacher. *Théorie des matrices, T2.* Dunod, 1966.

[Gob95a] Goblot. *Algèbre commutative.* Masson, 1995.

[Gob95b] Goblot. *Thèmes de géométrie.* Masson, 1995.

[Gou94a] X. Gourdon. *Les maths en tête, algèbre.* Ellipse, 1994.

[Gou94b] X. Gourdon. *Les maths en tête, analyse.* Ellipse, 1994.

[Goz97] Gozard. *Théorie de Galois.* Ellipses, 1997.

[GT96] Stéphane Gonnord and Nicolas Tosel. *Thème d'analyse pour l'agrégation, Calcul différentiel.* Ellipses, 1996.

[Kre99] Rainer Kress. *Linear integral equations.* Springer Verlag, 1999.

[LB88] Daniel Lehman and Rudolphe Bkouche. *Initiation à la géométrie.* PUF, 1988.

[Leb96] Leborgne. *Calcul différentiel complexe.* PUF, 1996.

[Mal00] Stéphane Mallat. *Une exploration des signaux en ondelettes.* Editions de l'école Polytechnique, 2000.

[Mig89] Maurice Mignotte. *Mathématiques pour le calcul formel*. PUF, 1989.

[Mne97] Rached Mneimné. *Eléments de géométrie*. Cassini, 1997.

[MT97] Rached Mneimné and Frédéric Testard. *Introduction à la théorie des groupes de Lie classiques*. Herman, 1997.

[Per95] Daniel Perrin. *Géométrie algébrique. Une introduction*. Inter Editions, 1995.

[Per96] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.

[PH89] A. Poli and LI Huguet. *Codes correcteurs, théorie et applications*. Masson, 1989.

[PW95] Odile Papini and Jacques Wolfman. *Algèbre discrète et codes correcteurs*. Springer Verlag, 1995.

[RDO79] Ramis, Deschamps, and Odoux. *Tome 1 : algèbre*. Masson, 1979.

[Rud87] Walter Rudin. *Analyse réelle et complexe*. Dunod, 1987.

[Sam67] Pierre Samuel. *Théorie des nombres*. Herman, 1967.

[Ser66] Jean-Pierre Serre. *Representations lineaires des groupes finis*. Herman, 1966.

[Ser70] Jean-Pierre Serre. *Cours d'arithmétique*. PUF, 1970.

[Sid98] Jean Claude Sidler. *Géométrie projective. Cours, exercices et problèmes corrigés*. Dunod, 1998.

[Tos99] Nicolas Tosel. *Une forme faible du théorème taubérien de Wiener-Ikehara*. RMS, 1999.

[Vid01] Romain Vidonne. *Groupe circulaire, rotations et quaternions*. Ellipses, 2001.

[War71] Warusfel. *Structures algébriques finies*. Hachette, 1971.

[Zis96] Michel Zisman. *Mathématiques pour l'agrégation*. Dunod, 1996.

[ZQ95] Zuily and Queffelec. *Eléments d'analyse pour l'agrégation*. Masson, 1995.

Index

élimination, 13, 17
équation aux classes, 14, 23
équation de Poisson, 11
équation différentielle, 27
équations aux dérivées partielles, 11
équations différentielles, 15, 22, 25, 27
équations diophantiennes, 19, 25
équations polynomiales, 13, 17, 21
équi-continuité, 28

action de groupe, 6, 14, 24
actions de groupe, 2, 7
algorithme, 22
algorithme d'Euclide, 19
algorithme du simplexe, 9
algorithme FFT, 11
algorithmes, 9, 11–13, 19, 21, 26
angles, 7, 12, 14
applications ouvertes, 8
approximation, 28
approximation des nombres réels, 19
arbres binaires, 22

barycentre, 23

cône convexe, 12
cônes, 10
calcul des coefficients de Fourier, 11
calcul différentiel, 12, 15, 25, 27
caractères, 6, 11
combinatoire, 22, 23
compacité, 2, 22, 23, 27
complexité, 26
comportement asymptotique, 21, 23
congruence, 24
coniques, 12, 14, 22, 25
connexité, 8
convexité, 2, 9, 12, 23
convolution, 15
corps fini, 13
corps finis, 15, 21
courbes, 22
cyclotomie, 13, 14, 24

décomposition, 26
décomposition polaire, 27
dénombrabilité, 21
dénombrement, 13
déterminant, 2, 17, 22, 26, 27
développement asymptotique, 28
dimension, 6
dimension finie, 28
division euclidienne, 7, 13, 19
droite projective, 7, 20
droites et cercles, 7
dualité, 7, 11–13, 24

enveloppe convexe, 27
espace L^2, 17
espace affine, 17
espace des flots, 15
espace hermitien, 6
espace projectif, 25
espaces complets, 28
espaces denses, 27
espaces projectifs, 25
exponentielle, 8, 25
exponentielle de matrices, 12
extémas, 20
extensions de corps, 14
extremum, 2

factorisation, 21
factorisation de matrices, 12
fonction ζ, 28
fonctions convexes, 12
fonctions holomorphes, 7, 28
fonctions méromorphes, 27
forme quadratique, 27
formes linéaires, 27
formes quadratiques, 9, 22
fractions rationnelles, 21

groupe cyclique, 11
groupe de permutations, 2
groupe fini, 11
groupe linéaire, 20, 21, 26
groupes, 23, 24
groupes finis, 6, 14, 24

groupes linéaire, 15
groupes symétrique, 24

homographies, 7, 20, 25, 26

idéal, 13, 21
idéaux, 23
intégrales dépendant d'un paramètre, 28
intégration numérique, 19
interpolation, 20
inversion locale, 8, 20, 25
isométrie, 17, 20
isométries, 8, 14, 24
itérations, 12, 21, 26

localisation, 25, 26

méthodes de quadrature, 28
méthodes de quadratures, 19
matrices, 27
matrices nilpotentes, 10, 20
matrices semblables, 2, 6, 7, 10
modules, 7

nombres premiers, 21, 24, 28

opérateurs compacts, 28
opérations élémentaires, 12
optimisation, 20, 22
orthogonalité, 22

parcours de graphes, 20
partie génératrice, 7, 21
parties génératrices, 23
plan hyperbolique, 23
point fixe, 2, 21, 26
points extrémaux, 9
polyèdre, 9
polyèdres, 24
polynôme, 9, 13, 15, 24
polynôme de meilleure approximation, 17
polynôme Lagrange, 20
polynômes, 11, 13, 17, 19, 21, 22, 25, 26
polynômes irréductibles, 13, 14
polynômes orthogonaux, 17, 28
produit hermitien, 6, 11
produit vectoriel, 8
programmation linéaire, 20

projection, 27, 28

quadriques, 10, 25
quaternions, 8

réduction d'endomorphismes, 7
réduction des endomorphismes, 25
réseau, 13, 27
réseaux, 7, 22
règle et compas, 12, 14
racines de l'unité, 11
racines de polynôme, 14, 25
racines de polynômes, 24–26
rang, 25
rang de matrices, 9, 13
relations de Newton, 9, 13

séparation des convexes, 12, 27
série de fonctions, 27
séries entières, 23
singularités, 19
sous groupes finis de $SO(3)$, 6
sous-espaces stables, 6, 12, 25
suite récurrente, 21
suites récurrentes, 26
symbole de Legendre, 21
systèmes différentiels linéaires, 12

théorème d'Ascoli, 28
théorème de Minkowski, 27
topologie, 23
transformée de Fourier, 11, 28
transformée de Laplace, 28
treillis, 21

valeurs propres, 12
variétés algébriques, 21
vissage, 8
vitesse de convergence, 19
volume, 2