Leçon n°101 : Groupe opérant sur un ensemble. Exemples et applications.

Soit G un groupe et X un ensemble non vide.

I - Opération d'un groupe sur un ensemble. [PER]

A - Premières définitions. [PER]

Définition 1 : Définition d'action de groupe.

Remarque 2 : Se donner une action revient à se donner un morphisme de groupe.

Définition 3 : Action transitive, fidèle.

Exemples 4 : $\mathfrak{S}_n$ agit transitivement et fidèlement sur $[\![1,n]\!]$, $\mathrm{GL}_n(\mathbb{C})$ agit transitivement et fidèlement sur $\mathbb{C}^n \backslash \{0\}$, $\mathrm{O}_n(\mathbb{R})$ agit transitivement sur $\mathbb{R}^n$.

Remarque 5 : Si G opère sur X alors $G/\mathrm{Ker}(\varphi)$ agit fidèlement sur X.

Remarque 6 : Soit E un $\mathbb{K}$-ev, pour l'action de $\mathrm{GL}(E)$ sur $\mathbb{P}(E)$, $\mathrm{Ker}(\varphi) = \mathrm{Z}(\mathrm{GL}(E)) = \mathbb{K}^\times Id_E$ et donc $\mathrm{PGL}(E)$ agit fidèlement sur $\mathbb{P}(E)$.

B/ Orbites et stabilisateurs. [PER]

Définition 7 : Relation $\mathcal{R}$: $x\mathcal{R}y \iff \exists g \in G,\ y = g\cdot x$

Définition 8 : Orbites.

Définition 9 : Stabilisateurs.

Proposition 10 : $\mathrm{Stab}(x)$ est un sous-groupe de G.

Remarque 11 : Être transitif c'est n'avoir qu'une seule orbite.

Remarque 12 : Les orbites pour l'action de $\mathrm{O}_n(\mathbb{R})$ sur $\mathbb{R}^n$ sont les sphères, dans celle de $\mathfrak{S}_n$ le stabilisateur d'un point est isomorphe à $\mathfrak{S}_{n-1}$.

C/ Dénombrer à l'aide des orbites. [PER] [ROM]

Proposition 13 : ${}^{G}/_{\mathrm{Stab}(x)}$ est en bijection avec $\omega(x)$.

Théorème 14 : Équation aux classes.

Développement 1

Application 15 : Dénombrement des endomorphismes diagonalisables de $\mathbb{F}_q^n$

Théorème 16 : Formule de Burnside.

Application 17 : Problème de la roulette : on se donne une roulette à n segments et c couleurs et on dit que deux roulettes ont la même coloration si l'on peut passer de l'une à l'autre après rotation de la roulette, il y a donc $\frac{1}{n}\sum_{d|n}\varphi(d)c^{\frac{n}{d}}$ colorations possibles.

II/ Actions sur les groupes finis

A/ Action par translation. [PER]

Définition 18 : Action par translation.

Remarque 19 : Cette action est simplement transitive et fidèle.

Application 20 : Théorème de Cayley.

B/ Action par conjugaison. [PER]

Proposition 21 : Action par conjugaison, centralisateur.

Remarque 22 : Principe de conjugaison.

Application 23 : Théorème de Wedderburn : Tout anneau à division fini est commutatif.

Application 24 : Le centre d'un p-groupe n'est pas réduit au neutre.

C/ Application aux théorèmes de Sylow. [PER]

Définition 25 : p-sous-groupe de Sylow.

Théorème 26 : Théorème de Sylow 1 : Existence des p-Sylows.

Théorème 27 : Théorème de Sylow 2 : Dénombrement des p-Sylows et ils sont tous conjugués.

Corollaire 28 : Un p-Sylow est unique ssi il est distingué.

Application 29 : Un sous-groupe d'ordre 63 n'est pas simple. Les groupes d'ordre pq avec p et q premiers distincts ne sont pas simples.

III/ Applications dans d'autres domaines des mathématiques.

A/ Isomorphismes exceptionnels. [CAL] [PER]

Définition 30 : Définition groupes projectifs linéaires.

Proposition 31 : Dénombrement sur les corps finis : $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathbb{P}^n(F_q)$, $\mathrm{SL}_n(\mathbb{F}_q)$, $\mathrm{PGL}_n(\mathbb{F}_q)$ et $\mathrm{PSL}_n(\mathbb{F}_q)$.

Lemme 32 : Si H est un sous-groupe d'indice n de $\mathfrak{S}_n$ alors $H \simeq \mathfrak{S}_{n-1}$.

Théorème 33 : Isomorphismes exceptionnels.

B/ En géométrie : Isométries préservant les polytopes. [CAL]

Définition 34 : On note $I_S(X)$ les isométries laissant stable X.

Proposition 35 : Triangle équilatéral $I_S(X) \simeq \mathfrak{S}_3$. Pour le polygone régulier c'est le groupe diédral.

Proposition 36 : Groupe isométries tétraèdre.

Développement 2

Proposition 37 : Détermination du groupe des isométries du cube et colorations des cubes à c couleurs.

C/ Actions sur les groupes de matrices. [ROM]

Proposition 38 : Action $(P, A) \mapsto PA$ et orbites (lien avec les opérations élémentaires, on agit ici sur les lignes de la matrice A)

Proposition 39 : Action $(P, A) \mapsto AP^{-1}$ et orbites (lien avec les opérations élémentaires, on agit ici sur les colonnes de la matrice A)

Proposition 40 : Il existe une unique matrice échelonnée réduite dans chaque orbite.

Proposition 41 : Action de Steinitz ($(P, Q, A) \mapsto PAQ$) et orbites.

Proposition 42 : Connexité et adhérence de ces orbites.

Proposition 43 : Action par conjugaison : $(P, A) \mapsto PAP^{-1}$.

Proposition 44 : Dans $\mathbb{C}$ l'orbite de M est fermée ssi M est diagonalisable.

Références :

— [PER] Perrin p. 13-20

— [ROM] Rombaldi 2nde édition p. 21 et p. 197

— [CAL] Caldéro Histoires hédonistes tome 1 p. 250-257, p. 264, p. 363 et p. 376

Exercices/Questions autour de la leçon 101 :

Exercice 1 : Quel est le nombre d'orbites de l'action par congruence $\mathrm{GL}_n(\mathbb{C}) \times S_n(\mathbb{C}) \to S_n(\mathbb{C})$? Quel représentant privilégié dans les orbites ?

Solution exercice 1 : Cela revient à considérer le théorème de réduction des formes quadratiques sur $\mathbb{C}$, il y a donc $n+1$ orbites. On a donc $S_n(\mathbb{C}) = \bigcup_{k=0}^{n} O_r$ où O_r est l'orbite de $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

Exercice 2 : Quelles sont les orbites de l'action par congruence sur $\mathbb{R}$?

Solution exercice 2 : Penser au théorème d'inertie de Sylvester, dans chaque orbite on a un représentant privilégié qui est $\begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{pmatrix}$ avec $p+q=r$ où r est le rang.

Exercice 3 : Quelles sont les orbites par l'action par conjugaison ?

Solution exercice 3 : Deux matrices sont semblables ssi elles ont les mêmes invariants de similitude (réduction de Frobenius).

Exercice 4 : Soit G fini tel que $\mathrm{Aut}(G)$ agit transitivement sur $G \backslash \{1\}$. Montrer que $Z(G) \neq \{1\}$.

Solution exercice 4 : La transitivité de l'action implique que les ordres de tous les éléments distinct de 1 sont égaux, notons o cet ordre commun. Pour p diviseur premier de $n = |G|$, on a qu'il existe un élément d'ordre p (théorème de Cauchy), donc $o = p$ puis $n = p$. Ainsi G est un groupe d'ordre p et on conclut par l'application 24.

Exercice 5 : Un groupe d'ordre 200 n'est pas simple.

Solution exercice 5 : $200 = 2^3 \times 5^2$, on compte les 5-Sylow, il n'y en a qu'un donc le 5-Sylow est distingué et un groupe d'ordre 200 n'est pas simple.

Exercice 6 : Classifier les groupes d'ordre p^2.

Solution exercice 6 : Ils sont tous abéliens et soit isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ ou isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. (Regarder le centre du groupe).

Exercice 7 : Soit p premier. Quel est l'ordre des p-Sylow de $\mathfrak{S}_p$?

Solution exercice 7 : $|\mathfrak{S}_p| = p! = p \times (p-1)!$, comme p ne divise pas $(p-1)!$ alors ils sont d'ordre p.

Exercice 8 : Combien $\mathfrak{S}_p$ contient de p-cycles ?

Solution exercice 8 : On les compte en faisant agir $\mathfrak{S}_p$ sur les p-cycles, c'est une action transitive et on obtient par la formule des classes : $(p-1)!$. (On peut aussi le compter à la main en faisant attention que deux p-cycles sont les mêmes si on passe de l'un à l'autre par permutation circulaire des éléments).

Exercice 9 : En déduire le nombre de p-Sylow de $\mathfrak{S}_p$.

Solution exercice 9 : Les sous-groupes d'ordre p premier sont cycliques dont les p-Sylow sont engendrés par les p-cycles (car pas d'autres éléments d'ordre p que les p-cycles car p premier). Le sous-groupe engendré par un p-cycle contient toutes ses puissances donc il y en $p-1$ différents dans chaque p-Sylow. On a donc $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow dans $\mathfrak{S}_p$.

Exercice 10 : Soit G un groupe d'ordre 15, combien a-t-il d'élements d'ordre 3 ? Et 5 ?

Solution exercice 10 : Il y a un unique 3-Sylow donc deux éléments d'ordre 3. Pareil pour 5 on a donc 4 éléments d'ordre 5 (Sylow cyclique car d'ordre un nombre premier).

Exercice 11 : Montrer que G d'ordre 15 est cyclique.

Solution exercice 11 : En effet, en comptant il reste nécessairement 8 éléments d'ordre 15.

Exercice 12 : Montrer que $O_2^+(\mathbb{R})$ agit transitivement sur le cercle unité de $\mathbb{R}^2$.

Solution exercice 12 : Oui si on prend deux points A et B on considère la rotation d'angle (OA, OB).

Exercice 13 : Démontrer que $O_3^+(\mathbb{R})$ agit transitivement sur la sphère unité de $\mathbb{R}^3$.

Solution exercice 13 : On prend deux points A et B sur la sphère unité. Soit P le plan contenant O, A et B et D la droite perpendiculaire à P passant par O. On considère alors la rotation d'axe D transformant A en B par la rotation d'angle (OA,OB). (Résultat prolongeable sur $O_n(\mathbb{R})$ en prenant comme espace stable un espace de dimension $n-2$)

Exercice 14 : Un groupe de 35 éléments agit sur un ensemble à 19 éléments sans fixer aucun d'entre eux. Combien y-a-t-il d'orbites ? Combien d'éléments contiennent-elles ?

Solution exercice 14 : Une orbite a un cardinal divisant 35. Comme ne fixe aucun d'entre eux, pas 1. Comme au plus de cardinal 19, la seule possibilité est que cela vaille 7 (disons qu'il y en a m) ou 5 (disons qu'il y en a n). Les orbites réalisant une réunion disjointe de l'ensemble à 19 éléments, on doit avoir $5n+7m=19$; la seule possibilité est $n=1$ et $m=2$. Il y a donc 3 orbites, l'une à 5 éléments, les deux autres à 7 éléments.

Exercice 15 : Montrer qu'un groupe de cardinal 6 non abélien est isomorphe à $\mathfrak{S}_3$.

Solution exercice 15 : On compte les 3-Sylows et 2-Sylows sachant qu'il n'y a pas d'élément d'ordre 6. Ensuite un élément d'ordre 3 ne commute pas avec un élément d'ordre 2 car sinon le produit est d'ordre 6. On crée donc un morphisme envoyant un élément d'ordre 2 de G sur une transposition de $\mathfrak{S}_3$ et de même pour l'ordre 3.

Exercice 16 : Montrer qu'un sous-groupe d'ordre 30 possède un sous-groupe distingué non trivial.

Solution exercice 16 : $30=2\times 3\times 5$. Par le deuxième théorème de Sylow $n_2 \in \{1,3,5,15\}$, $n_3 \in \{1,10\}$ et $n_5 \in \{1,6\}$. Supposons qu'aucun des trois ne soit 1, on suppose alors que $n_2=3$, $n_3=10$ et $n_5=6$. Or 2,3 et 5 sont premiers donc les Sylows sont tous cycliques et d'intersection neutre (sinon ils sont tous égaux). On compte alors le nombre d'éléments du groupe G dans cette configuration : 1 (neutre) $+\,3\times 1$ (éléments engendrant un 2-Sylow) $+\,10\times 2+6\times 4>30$ c'est absurde et donc au moins un des trois est 1, un groupe d'ordre 30 n'est donc pas simple.

Exercice 17 : Montrer qu'un groupe d'ordre 35 est cyclique.

Solution exercice 17 : On regarde les Sylow, il n'y a qu'un seul 3-Sylow S_3 et un seul 5-Sylow S_5, l'intersection est réduite au neutre, ils sont cycliques et x_5 (générateur de S_5) et x_7 (générateur de S_7) commutent alors on factorise l'application $(k,l)\mapsto x_5^k x_7^l$ et on obtient le résultat avec le théorème chinois.

Exercice 18 : Montrer qu'un groupe de cardinal 255 admet au moins 3 sous-groupes distingués.

Solution exercice 18 : On regarde les Sylows, il y a un seul 17-Sylow. Pour les deux autres au moins un des deux vaut 1 sinon trop d'élément disons que $n_3=1$. On introduit $K=<S_{17},S_3>$ le sous-groupe engendré et il convient comme 3ème sous-groupe distingué.

Exercice 19 : Montrer que tout groupe d'ordre 48 admet un sous-groupe distingué d'ordre 8 ou 16.

Solution exercice 19 : $48=3\times 2^4$. Le nombre de 2-sous-groupes de Sylow divise 3 et est impair. S'il est égal à 1, G possède un sous-groupe distingué d'ordre 16. Le quotient de G par le sous-groupe distingué d'ordre 16 est alors isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Sinon, G a 3 sous-groupes de Sylow d'ordre 16. L'opération de G sur l'ensemble des 3-sous-groupes de Sylow par conjugaison est transitive et définit un morphisme $G\to\mathfrak{S}_3$. L'image est d'ordre 3 ou 6. En effet, si l'image est d'ordre 2, l'action ne peut pas être transitive. Le noyau qui est distingué est donc d'ordre $8=\frac{48}{6}$ ou $16=\frac{48}{3}$ (en fait le dernier cas, n'est pas possible car cela signifierait qu'il y a un sous-groupe de Sylow distingué, ce qui est contradictoire avec l'hypothèse faite). On a donc montré le résultat.

Exercice 20 : Les groupes de cardinaux pqr ne sont pas simples.

Solution exercice 20 : Si G n'a pas de sous-groupe distingué, les nombres n_p, n_q et n_r sont strictement supérieurs à 1. On a $n_r|pq$ et $n_r\equiv 1[r]$. Donc si n_r est différent de 1, il est de la forme $1+rk$ avec $k>0$ et divise pq. Comme r est plus grand que p et q, il ne peut être égal à p ou q. Donc, il y aurait pq r-sous-groupes de Sylow. Il y aurait alors $pq(r-1)$ éléments d'ordre r. De même, n_p|qr, donc $n_p\geq q$ et $n_q|pr$ et $n_p\geq p$. Il y aurait donc au moins $q(p-1)$ éléments d'ordre p et $p(q-1)$ éléments d'ordre q. Ce qui donne au moins $pq(r-1)+q(p-1)+p(q-1)+1=pqr+(q-1)(p-1)$ éléments, ce qui est plus que pqr. Donc un des entiers n_p, n_q ou n_r est égal à 1.

Exercice 21 : Soit G un groupe non abélien et Z son centre. Montrer que G/Z n'est pas monogène.

Solution exercice 21 : Montrons la réciproque. Supposons a générateur de G/Z alors si $x,y \in G$ on a $x = a^k g$ et $y = a^l g'$ où $(k,l) \in \mathbb{N}$ et $g,l \in Z$. Alors $xy = a^k g a^l g' = a^{k+l} g g' = a^l g' a^k g = yx$ donc G abélien.

Exercice 22 : Dénombrer le nombre de sous-espaces vectoriels de dimension r de $(\mathbb{F}_q)^n$.

Solution exercice 22 : Considérons ensuite l'action $\mathrm{GL}_n(\mathbb{F}_q) \times V_r \to V_r, (M,F) \mapsto MF$ où V_r est l'ensemble des sous-espaces vectoriels de dimension r. L'action est transitive (penser aux matrices de passage d'une base complétée de l'un sur une base complétée de l'autre). Calculons $|\mathrm{Stab}(V)|$ où $V \in V_r$. En se plaçant dans la bonne base, on voit que $M \in \mathrm{Stab}(V) \iff \begin{pmatrix} M_V & \star \\ 0 & M_U \end{pmatrix}$ où $M_V \in \mathrm{GL}_r(\mathbb{F}_q)$ et $M_U \in \mathrm{GL}_{n-1}(\mathbb{F}_q)$. Donc $|\mathrm{Stab}(V)| = |\mathrm{GL}_r(\mathbb{F}_q)||\mathrm{GL}_{n-r}(\mathbb{F}_q)|q^{r(n-r)}$ et l'équation aux classes donne le résultat.

Exercice 23 : Dénombrer le nombre de k-cycles de $\mathfrak{S}_n$.

Solution exercice 23 : On fait agir $\mathfrak{S}_n$ sur les k-cycles par conjugaison cette action est transitive on cherche donc juste le stabilisateur d'un élément k-cycle. On a $\sigma \in \mathrm{Stab}((a_1,\ldots,a_n))$ ssi $\sigma(a_1)$ à choisir et le reste ne bouge pas. Donc $|\mathrm{Stab}((a_1,\ldots,a_n))| = k \times (n-k)!$, on déduit le résultat de l'équation aux classes.

Exercice 24 : Déterminer l'ensemble des isométries laissant stable un octaèdre. De même pour le dodécaèdre et l'icosaèdre.

Solution exercice 24 : Fait proprement dans Caldéro Histoires hédonistes tome 1. L'octaèdre est le dual du cube et a donc le même groupe d'isométries que le cube. On peut inscrire 5 cubes dans le dodécaèdre et faire agir sur ces cinq cubes. L'icosaèdre est le dual du dodécaèdre et a donc le même groupe d'isométries que le dodécaèdre.

Leçon n° 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.

I/ De l'exponentielle complexe au groupe $\mathbb{U}$.

A/ Autour de l'exponentielle. [T] [ARN]

Définition 1 : $\mathbb{U}$.

Définition 2 : Exponentielle complexe.

Proposition 3 : Prop de l'exponentielle complexe et lien avec $\mathbb{U}$ sur ses props.

Proposition 4 : exp morphisme surjectif de $(\mathbb{C}, +)$ dans $(C^*, \times)$ et de noyau $2i\pi\mathbb{Z}$.

Théorème 5 : Homéomorphisme surjectif de groupe de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$ et non injectif.

Proposition 6 : Formule d'Euler et de Moivre.

Proposition 7 : $\cos^2 + \sin^2 = 1$, lien géométrique entre $\cos(\theta)$, $\sin(\theta)$ et $e^{i\theta}$ avec annexe.

Application 8 : Linéarisation de $\cos^n(\theta)$ et $\sin^n(\theta)$.

Application 9 : Polynômes de Tchébychev.

Application 10 : Calcul noyaux de Dirichlet et Féjer.

Théorème 11 : $\begin{array}{cccc} \varphi & : & \mathbb{R}^{+*} \times \mathbb{U} & \to & \mathbb{C}^* \\ & & (r, e^{i\theta}) & \mapsto & re^{i\theta} \end{array}$ est un isomorphisme.

B/ Groupe des racines n-ièmes de l'unité. [PER] [ARN] [G]

Définition 12 : Racines n-ièmes.

Proposition 13 : Expression ensembliste de $\mathbb{U}_n$ et groupe cyclique d'ordre n.

Exemple 14 : Représenter graphiquement $\mathbb{U}_4$, $\mathbb{U}_5$ et $\mathbb{U}_8$.

Théorème 15 : Le seul sous-groupe fini de $(\mathbb{C}^*, \times)$ d'ordre n est $\mathbb{U}_n$.

Définition 16 : Racines primitives n-ièmes de l'unité.

Proposition 17 : Ensemble des racines primitives n-ièmes.

Définition 18 : Indicatrice d'Euler.

Proposition 19 : $\mathbb{U}_n = \bigcup\limits_{d|n} \mathbb{U}_d^*$.

Application 20 : $n = \sum\limits_{d|n} \varphi(d)$.

Théorème 21 : [FGNAlg1] Gauss-Lucas.

Application 22 : Son application avec les racines de l'unité.

Développement 1

Lemme 23 : Déterminant circulant.

Application 24 : Suite de polygones.

II/ Notion d'angles orientés et argument.

A/ Angles orientés et argument d'un nombre complexe. [ARN] [T] [AUD]

Définition 25 : Un argument de z.

Proposition 26 : Ensemble des arguments de z.

Définition 27 : Argument principal et lien avec dét principale du logarithme.

Théorème 28 : Il n'existe pas de dét continue de l'argument sur $\mathbb{C}$.

Proposition 29 : Notion d'angle orienté de deux vecteurs unitaires.

Proposition 30 : Un argument d'un nombre complexe z est une mesure d'angle formé par $\overrightarrow{i}$ et du vecteur d'affixe $\frac{z}{|z|}$.

B/ Rotation et groupe diédral. [ROM]

Définition 31 : Rotation d'angle θ autour de 0 : $r_\theta : z \mapsto e^{i\theta} z$.

Proposition 32 : Elles laissent $\mathbb{U}$ stable.

Application 33 : Groupe diédral (groupe des isométries laissant stable le polygone régulier à n côtés).

III/ Application aux polynômes cyclotomiques.

A/ Définitions et propriétés. [PER]

Définition 34 : Polynôme cyclotomique.

Proposition 35 : $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Exemple 36 : Calcul de Φ_3, Φ_4 et Φ_8.

Proposition 37 : $\Phi_n(X) \in \mathbb{Z}[X]$ unitaire.

Développement 2

Théorème 38 : Irréductibilité des polynômes cyclotomiques.

Corollaire 39 : $[\mathbb{Q}(e^{\frac{2i\pi}{n}}) : \mathbb{Q}] = \varphi(n)$.

Application 40 : Une extension finie $\mathbb{K}$ de $\mathbb{Q}$ admet un nombre fini de racines de l'unité.

Corollaire 41 : Soit α (resp. β) une racine n (resp. m)-ième primitive de l'unité alors si $m \wedge n = 1$ alors $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$.

B/ Applications. [PER] [FGNAlg1]

Application 42 : Théorème de Wedderburn.

Application 43 : Théorème de Kronecker.

Corollaire 44 : Soit $P \in Z[X]$ unitaire de degré n et irréductible sur $\mathbb{Q}$. Si toutes les racines de P sont de module inférieur ou égal à 1, alors $P = X$ ou $P = \Phi_n$.

Références :

— [PER] Perrin p. 80
— [ROM] Rombaldi 2nde édition p. 83
— [ARN] Arnaudiès Cours de mathématiques Tome 1 p. 247
— [T] Tauvel Analyse complexe pour la licence p. 58 et p. 62
— [AUD] Audin Géométrie p. 73
— [FGNAlg1] Francinou, Gianella, Nicolas Algèbre tome 1 p. 213 et p. 229
— [G] Gourdon Algèbre p. 146

Leçon n° 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

Dans toute la suite on considérera G un groupe.

I/ Conjugaison dans un groupe.

A/ Action par conjugaison. [U] [PER]

Définition 1 : Action par conjugaison.

Définition 2 : Classes de conjugaison, conjugués.

Exemple 3 : Les classes de conjugaison d'un groupe abélien sont triviales.

Exemple 4 : Dans $\mathfrak{S}_n$, les p-cycles sont conjugués.

Exemple 5 : Si $A, B \in \mathrm{GL}_n(\mathbb{K})$ A et B sont conjugués ssi semblables.

Définition 6 : Centralisateur.

Application 7 : Théorème de Wedderburn : tout anneau à division fini est commutatif.

B/ Étude de quelques classes de conjugaison. [U] [PER] [G]

Remarque 8 : Principe de conjugaison de Perrin : un élément conjugué est du même type qu'un élément de départ.

Exemple 9 : La conjugaison conserve l'ordre dans un groupe + si $s_D \in \mathrm{SO}_3(\mathbb{R})$ rotation d'axe D et $\varphi \in \mathrm{O}_3(\mathbb{R})$ alors $\varphi \circ \sigma_D \circ \varphi^{-1} = s_{\varphi(D)}$ rotation d'axe $\varphi(D)$.

Théorème 10 : Décomposition des éléments de $\mathfrak{S}_n$.

Définition 11 : Type d'une permutation.

Théorème 12 : Deux permutations sont conjuguées ssi elles ont même type.

Exemple 13 : $(1\ 2\ 3)(4\ 5)$ et $(1\ 3\ 4)(2\ 5)$ sont conjuguées par $\sigma = (2\ 3\ 4\ 5)$

Théorème 14 : Réduction de Frobenius.

Proposition 15 : $u,v \in \mathcal{L}(E)$ sont conjuguées ssi ont les mêmes facteurs invariants.

II/ Sous-groupes stables par conjugaison.

A/ Sous-groupes distingués. [U] [PER]

Définition 16 : Sous-groupes distingués.

Exemple 17 : $\{1\}$ et G sont distingués.

Exemple 18 : Si G abélien tous ces sous-groupes sont distingués, réciproque fausse avec $\mathbb{H}_8$ le groupe des quaternions : tout ces sous-groupes sont distingués mais il n'est pas abélien.

Proposition 19 : Image directe et réciproque d'un distingué.

Exemple 20 : $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$, de même pour SL_n dans GL_n.

Proposition 21 : Si $K \subset H \subset G$ et K distingué dans G alors K distingué dans H.

Contre-exemple 22 : Le groupe $\langle(1\ 2)(3\ 4)\rangle$ est distingué dans $V_4 = \{\mathrm{Id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ et V_4 est distingué dans $\mathfrak{A}_4$ et pourtant $\langle(1\ 2)(3\ 4)\rangle$ n'est pas distingué dans $\mathfrak{A}_4$.

B/ Groupes quotients. [U] [PER]

Définition 23 : Classes à gauche, droite, indice.

Proposition 24 : Les classes ont même cardinal que l'indice.

Théorème 25 : Théorème de Lagrange.

Proposition 26 : Si un sous-groupe est d'indice 2 alors il est distingué.

Application 27 : $\mathfrak{A}_4$ ne possède pas de sous-groupe d'ordre 6.

Théorème 28 : Construction des groupes quotients par factorisation.

Exemple 29 : Construction de $\mathbb{Z}/n\mathbb{Z}$, $\mathrm{PGL}_n(\mathbb{K})$ et $\mathrm{PSL}_n(\mathbb{K})$.

Définition 30 : Sous-groupe dérivé.

Théorème 31 : Abélianisé d'un groupe.

Exemple 32 : $D(\mathfrak{A}_4) = V_4$.

C/ Théorèmes d'isomorphismes. [U]

Théorème 33 : 1er théorème d'isomorphisme.

Application 34 : Les groupes cycliques d'ordre n sont isomorphes à $\mathbb{Z}/n\mathbb{Z}$.

Théorème 35 : 2ème théorème d'isomorphisme.

III/ Applications de la conjugaison.

A/ Cas des groupes simples et p-groupes. [U] [PER] [ROM]

Définition 36 : Groupe simple.

Exemple 37 : $\mathbb{Z}/n\mathbb{Z}$ simple ssi n premier.

Développement 1

Lemme 38 : Les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Théorème 39 : $\mathfrak{A}_n$ est simple pour $n \geq 5$.

Corollaire 40 : Les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.

Définition 41 : p-groupes.

Proposition 42 : Les p-groupes ont un centre non trivial.

Corollaire 43 : Les groupes d'ordre p^2 sont toujours abéliens.

B/ Isomorphismes exceptionnels. [CAL]

Développement 2

Proposition 44 : Dénombrement sur les corps finis : $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathbb{P}^n(F_q)$, $\mathrm{SL}_n(\mathbb{F}_q)$, $\mathrm{PGL}_n(\mathbb{F}_q)$ et $\mathrm{PSL}_n(\mathbb{F}_q)$.

Lemme 45 : Si H est un sous-groupe d'indice n de $\mathfrak{S}_n$ alors $H \simeq \mathfrak{S}_{n-1}$.

Théorème 46 : Isomorphismes exceptionnels.

Références :

— [PER] Perrin p. 10, p. 15 et p. 82
— [U] Ulmer Théorie des groupes p. 5, p. 33, p. 45 et p. 57
— [G] Gourdon Algèbre p. 291
— [ROM] Rombaldi Algèbre 2nd éd. p. 50
— [CAL] Caldéro Histoires hédonistes tome 1 p. 250

Leçon n° 104 : Groupes finis. Exemples et applications.

Soit G un groupe fini.

I/ Propriétés sur les groupes et classification des groupes abéliens finis.

A/ Premières définitions et propriétés. [PER] [ROM]

Définition 1 : Ordre d'un groupe.

Définition 2 : Classe à gauche et indice.

Théorème 3 : Lagrange.

Corollaire 4 : $|G| = [G : H]|H|$.

Remarque 5 : Réciproque fausse $\mathfrak{A}_4$ n'admet pas de sous-groupe d'ordre 6.

Définition 6 : Générateurs d'un groupe.

Définition 7 : Ordre d'un élément.

Proposition 8 : Propriétés sur l'ordre d'un élément.

Définition 9 : Sous-groupe distingué.

Proposition 10 : Quotient et structure de groupe.

Application 11 : Construction de $\mathbb{Z}/n\mathbb{Z}$.

Définition 12 : Groupe simple.

B/ Groupes cycliques. [ROM]

Définition 13 : Groupe monogène et cyclique.

Exemple 14 : $\mathbb{U}_n$ et $\mathbb{Z}/n\mathbb{Z}$.

Proposition 15 : Un groupe de cardinal premier est cyclique.

Proposition 16 : Tout groupe cyclique est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Proposition 17 : La réciproque du théorème de Lagrange est vraie pour les groupes cycliques.

C/ Le cas de $\mathbb{Z}/n\mathbb{Z}$. [ROM]

Proposition 18 : Éléments engendrant $\mathbb{Z}/n\mathbb{Z}$.

Définition 19 : Indicatrice d'Euler.

Proposition 20 : Il y a $\varphi(d)$ générateurs d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.

Application 21 : Tout sous-groupe fini d'un corps multiplicatif est cyclique.

Théorème 22 : Théorème chinois.

D/ Classification des groupes abéliens finis. [ROM]

Théorème 23 : Théorème de structure des groupes abéliens finis.

Application 24 : Avec le théorème chinois, on les a tous à isomorphisme près.

Exemple 25 : Groupes d'ordre 24 à isomorphismes près.

II/ Exemples de groupes finis non abéliens : $\mathfrak{S}_n$ et $\mathfrak{A}_n$. [ROM]

Définition 26 : Groupe symétrique $\mathfrak{S}_n$.

Proposition 27 : Son cardinal.

Théorème 28 : Décomposition en produit de cycles disjoints.

Théorème 29 : Systèmes de générateurs de $\mathfrak{S}_n$.

Proposition 30 : Existence et unicité du morphisme signature.

Définition 31 : Groupe alterné : unique sous-groupe d'indice 2 dans $\mathfrak{S}_n$.

Développement 1

Lemme 32 : Les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Théorème 33 : $\mathfrak{A}_n$ est simple pour $n \geq 5$.

Corollaire 34 : Les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.

III/ Action de groupes : outil pour l'étude des groupes finis.

A/ Action de groupe. [PER]

Définition 35 : Action de groupe.

Remarque 36 : Pareil que de se donner un morphisme.

Application 37 : Théorème de Cayley.

Définition 38 : Stabilisateur et orbite.

Théorème 39 : Équation aux classes.

Application 40 : Tout groupe d'ordre p^2 est abélien.

Théorème 41 : Formule de Burnside.

B/ Sous-groupes de Sylow. [PER]

Définition 42 : p-sous-groupe de Sylow.

Théorème 43 : Théorème de Sylow 1 : Existence des p-Sylows.

Théorème 44 : Théorème de Sylow 2 : Dénombrement des p-Sylows et ils sont tous conjugués.

Corollaire 45 : Un p-Sylow est unique ssi il est distingué.

Application 46 : Un sous-groupe d'ordre 63 n'est pas simple. Les groupes d'ordre pq avec p et q premiers distincts ne sont pas simples.

C/ En géométrie : Isométries préservant les polytopes. [CAL]

Définition 47 : On note $I_S(X)$ les isométries laissant stable X.

Proposition 48 : Triangle équilatéral $I_S(X) \simeq \mathfrak{S}_3$. Pour le polygone régulier c'est le groupe diédral.

Proposition 49 : Groupe isométries tétraèdre.

Développement 2

Proposition 50 : Détermination du groupe des isométries du cube et colorations des cubes à c couleurs.

Références :

— [PER] Perrin p. 9
— [ROM] Rombaldi Algèbre 2nd éd. p.1, p. 26, p. 37 et p. 279
— [CAL] Caldéro Histoires hédonistes tome 1 p. 250

Leçon n° 105 : Groupe de permutations d'un ensemble fini. Applications

Dans la suite on prendra E un ensemble fini de cardinal $n \geq 1$.

I/ Le groupe symétrique $\mathfrak{S}_n$.

A/ Définitions et premières propriétés. [ROM] [PER]

Définition 1 : On note $\mathfrak{S}(E)$.

Proposition 2 : Groupe et cardinal.

Proposition 3 : Si E et F sont isomorphes alors $\mathfrak{S}(E)$ et $\mathfrak{S}(F)$ aussi.

Théorème 4 : Théorème de Cayley.

Remarque 5 : On se ramène à l'étude de $\mathfrak{S}_n$.

Définition 6 : r-cycle.

Définition 7 : Transposition.

Exemple 8 : Exemples de cycles.

Proposition 9 : Un r-cycle est d'ordre r.

Proposition 10 : Centre de $\mathfrak{S}_n$ est réduit à l'identité pour $n \geq 3$.

B/ Actions, support et orbites. [U]

Définition 11 : Points fixes.

Définition 12 : Support.

Proposition 13 : Lien entre support et produit de permutation.

Théorème 14 : Décomposition des permutations en produit de cycles à supports disjoints.

Exemple 15 : Exemple de décomposition.

Définition 16 : Type d'une permutation.

Proposition 17 : Lien entre ordre d'une permutation et type.

Exemple 18 : Reprendre exemple précédent et donner son ordre et son type.

C/ Classes de conjugaison. [U] [ROM]

Proposition 19 : Conjugué d'un k-cycle : $\sigma(a_1 \ \dots \ a_k)\sigma^{-1} = (\sigma(a_1) \ \dots \ \sigma(a_k))$

Application 20 : Calcul du nombre de k-cycles en utilisant la transitivité de l'action conjugaison sur les k-cycles.

Proposition 21 : Deux permutations sont conjuguées ssi elles ont même type.

D/ Générateurs. [ROM] [PGCD]

Proposition 22 : Tout r-cycle s'écrit comme produit de $r-1$ transpositions.

Théorème 23 : Les transpositions engendrent $\mathfrak{S}_n$.

Application 24 : Théorème de Schwarz (On montre que le théorème est vrai pour les transpositions et donc est vrai partout)

Proposition 25 : Autres systèmes de générateurs de $\mathfrak{S}_n$.

II/ Morphisme signature et groupe alterné.

A/ Signature d'une permutation. [U] [ROM]

Définition 26 : Existence et unicité du morphisme de signature.

Proposition 27 : Calcul de la signature dans certains cas (transpositions et type).

Définition 28 : Groupe alterné.

Proposition 29 : $\mathfrak{A}_n$ est l'unique sous-groupe distingué d'indice 2 dans $\mathfrak{S}_n$.

B/ Structure de $\mathfrak{A}_n$ et $\mathfrak{S}_n$. [ROM] [PER]

Développement 1.a)

Proposition 30 : $\mathfrak{A}_n$ est engendré par les 3-cycles.

Théorème 31 : $\mathfrak{A}_n$ est simple pour $n \geq 5$.

Remarque 32 : $\mathfrak{A}_4$ n'est pas simple (V_4 est un sous-groupe non trivial distingué).

Corollaire 33 : Groupes dérivés de $\mathfrak{A}_n$ et $\mathfrak{S}_n$.

Remarque 34 : Groupe dérivé de $\mathfrak{A}_4$.

Développement 1.b)

Corollaire 35 : Les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.

Corollaire 36 : Si H sous-groupe de $\mathfrak{S}_n$ d'indice n alors $H \simeq \mathfrak{S}_{n-1}$.

Application 37 : Isomorphismes exceptionnels.

III/ Applications à d'autres domaines des mathématiques.

A/ Matrices et permutation. [ROM] [OBJ] [PER]

Définition 38 : Matrice de permutation.

Proposition 39 : Morphisme injectif entre $\mathfrak{S}_n$ et $\mathrm{GL}_n(\mathbb{R})$ (via les matrices de permutation).

Corollaire 40 : Tout groupe fini d'ordre $n \geq 1$ où p premier divise n alors il est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$.

Remarque 41 : Utile pour la preuve du premier théorème de Sylow : soit G un groupe, on l'injecte dans $\mathfrak{S}_n$ via Cayley puis on l'injective dans $\mathrm{GL}_n(\mathbb{F}_p)$. Il suffit après d'expliciter un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$ et de redescendre.

Théorème 42 : Frobenius-Zolotarev.

B/ Polynômes symétriques. [GOU]

Définition 43 : Polynôme symétrique sur un anneau commutatif.

Exemple 44 : $X + Y + Z \in \mathbb{Z}[X, Y, Z]$ est symétrique.

Définition 45 : Polynômes symétriques élémentaires.

Application 46 : Relations coefficients-racines.

Théorème 47 : Théorème de décomposition des polynômes symétriques.

Exemple 48 : $X^2 + Y^2 + Z^2 = (X + Y + Z)^2 - 2(XY + XZ + YZ)$.

Application 49 : Théorème de Kronecker.

C/ En géométrie : Isométries préservant les polytopes. [CAL]

Définition 50 : On note $I_S(X)$ les isométries laissant stable X.

Proposition 51 : Triangle équilatéral $I_S(X) \simeq \mathfrak{S}_3$. Pour le polygone régulier c'est le groupe diédral.

Proposition 52 : Groupe isométries tétraèdre.

Développement 2

Proposition 53 : Détermination du groupe des isométries du cube et colorations des cubes à c couleurs.

Références :

— [PER] Perrin p. 18
— [ROM] Rombaldi Algèbre 2nd éd. p. 37-44, p. 407 et p. 429
— [U] Ulmer Théorie des groupes p. 46, p. 55-59
— [PGCD] Rouvière Petit guide du calcul différentiel p. 284
— [G] Gourdon Algèbre p. 78
— [OBJ] Beck, Malick Peyré Objectif Agrégation p. 251
— [CAL] Caldéro Histoires hédonistes tome 1 p. 250

Leçon n° 106 : Groupe linéaire d'un espace vectoriel de dimension finie. Sous-groupes de GL(E). Applications.

Dans toute la suite on prendra $\mathbb{K}$ un corps et E un $\mathbb{K}$-ev de dimension finie $n \geq 1$.

I/ Généralités sur le groupe linéaire. [PER] [ROM] [FGNAlg2]

Définition 1 : Définition du groupe linéaire.

Remarque 2 : Si $\mathcal{B}$ est une base de E, il existe un isomorphisme non canonique entre $\mathrm{GL}(E)$ et $\mathrm{GL}_n(\mathbb{K})$. L'intérêt est de fournir un outil pour le calcul matriciel.

Proposition 3 : Le déterminant est un morphisme de groupe, on définit $\mathrm{SL}(E)$.

Remarque 4 : Comme précédemment, $\mathrm{SL}(E)$ et $\mathrm{SL}_n(\mathbb{K})$ sont isomorphes non canoniquement.

Proposition 5 : Définitions équivalentes d'une dilatation.

Remarque 6 : Définition des matrices de dilatation.

Proposition 7 : Définitions équivalentes d'une transvection.

Remarque 8 : Définition des matrices de transvection.

Développement 1.a)

Théorème 9 : Les transvections engendrent $\mathrm{SL}_n(\mathbb{K})$.

Corollaire 10 : Les transvections et dilatations engendrent $\mathrm{GL}_n(\mathbb{K})$.

Application 11 : (Algorithme du pivot de Gauss et opérations élémentaires) + complexité.

Proposition 12 : (Comportement par conjugaison).

Proposition 13 : Deux dilatations sont conjuguées ssi elles ont même rapport.

Proposition 14 : Deux transvections quelconques sont conjuguées dans $\mathrm{GL}(E)$. Et si $n \geq 3$ elles le sont aussi dans $\mathrm{SL}(E)$.

II/ Étude des groupes GL(E) et SL(E).

A/ Centres et groupes dérivés. [PER]

Lemme 15 : Les éléments de $\mathrm{GL}(E)$ laissant stable toute droite sont les homothéties.

Proposition 16 : Centre de $\mathrm{GL}(E)$ et $\mathrm{SL}(E)$.

Proposition 17 : Groupe dérivé de $\mathrm{GL}_n(\mathbb{K})$ et $\mathrm{SL}_n(\mathbb{K})$.

B/ Cardinaux et isomorphismes exceptionnels. [PER] [CAL]

Définition 18 : Groupes projectifs linéaires (et spécial linéaire).

Proposition 19 : L'action du groupe projectif sur les droites est fidèle.

Proposition 20 : Cardinaux des différents objets.

Théorème 21 : Isomorphismes exceptionnels.

Développement 2

Théorème 22 : Dénombrement des endomorphismes diagonalisables de $\mathbb{F}_q^n$.

C/ Matrices et permutations. [ROM] [OBJ]

Définition 23 : Matrices de permutation.

Proposition 24 : Morphismes entre $\mathfrak{S}_n$ et $\mathrm{GL}_n(\mathbb{R})$.

Corollaire 25 : Tout groupe fini d'ordre $n \geq 1$ est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$ où p est premier.

Théorème 26 : Frobenius-Zolotarev.

D/ Groupe orthogonal. [BER] [ROM] [CAL]

Définition 27 : Groupe orthogonal et groupe unitaire.

Proposition 28 : Ce sont des sous-groupes de $\mathrm{GL}(E)$.

Définition 29 : Isométrie directe et groupe spécial orthogonal.

Proposition 30 : Si u est une isométrie (dans $\mathbb{R}$) alors il existe des espaces de dimension au plus 2 en somme directe stables par u.

Théorème 31 : (Réduction des isométries).

Théorème 32 : Décomposition polaire.

III/ Autres résultats sur GL(E).

A/ Actions de groupes matriciels. [ROM]

Proposition 33 : Action $(P, A) \mapsto PA$ et orbites.

Proposition 34 : Action $(P, A) \mapsto AP^{-1}$ et orbites.

Proposition 35 : Action de Steinitz (par équivalence) et orbites.

Proposition 36 : Action de $\mathrm{GL}(E)$ sur les espaces vectoriels de dimension k permettant de dénombrer cet ensemble si E et $\mathbb{K}$ sont finis.

B/ Topologie du groupe linéaire [ROM] [FGNAlg2]

On se place ici dans le cas où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Théorème 37 : $\mathrm{GL}(E)$ est ouvert dans $\mathcal{L}(E)$.

Théorème 38 : $\mathrm{GL}(E)$ est dense et $u \mapsto u^{-1}$ est continue.

Proposition 39 : $\mathrm{SL}(E)$ est fermé.

Proposition 40 : $\mathrm{GL}_n(\mathbb{C})$ est connexe.

Développement 1.b)

Proposition 41 : $\mathrm{SL}_n(\mathbb{K})$ est connexe par arcs.

Proposition 42 : $\mathrm{GL}_n(\mathbb{R})$ n'est pas connexe mais admet deux composantes connexes $\mathrm{GL}_n^+(\mathbb{R})$ et $\mathrm{GL}_n^-(\mathbb{R})$.

Références :

— [PER] Perrin p. 95
— [ROM] Rombaldi Algèbre 2nd éd. p. 139, p. 183 et p. 407
— [OBJ] Beck, Malick Peyré Objectif Agrégation p. 251
— [CAL] Caldéro Nouvelles Histoires hédonistes tome 1 p. 347 et Caldéro Histoires hédonistes tome 1 p. 250
— [FGNAlg2] Francinou Gianella Nicolas Algèbre 2 p. 177

Leçon n° 108 : Exemples de parties génératrices d'un groupe. Applications.

Soit G un groupe.

I/ Parties génératrices de groupes.

A/ Préambule. [PER]

Définition 1 : Définition de partie générée par une partie A et partie génératrice.

Définition 2 : Groupes de type fini.

Exemple 3 : $\mathbb{Z}$ est de type fini, pas $\mathbb{Q}$, tout groupe fini est de type fini.

Définition 4 : Groupe dérivé.

Proposition 5 : Abélianisé.

B/ Groupes monogènes et cycliques, cas de $\mathbb{Z}/n\mathbb{Z}$. [PER] [ROM]

Définition 6 : Monogène, cyclique.

Proposition 7 : Si G est d'ordre premier, G est cyclique.

Proposition 8 : $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n et ses générateurs sont les $\overline{k}$ pour $k \wedge n = 1$.

Corollaire 9 : $\mathbb{Z}/n\mathbb{Z}$ possède donc $\varphi(d)$ générateurs d'ordre $d|n$ où φ est l'indicatrice d'Euler.

Application 10 : Tout sous-groupe fini d'un corps multiplicatif est cyclique.

Application 11 : $\mathbb{F}_q^\times$ est cyclique.

Proposition 12 : Si G monogène infini, alors $G \simeq \mathbb{Z}$; si G cyclique, alors $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Proposition 13 : Les sous-groupes d'un groupe cyclique sont cycliques.

Proposition 14 : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique ssi $n = 2, 4, p^\alpha, 2p^\alpha$

C/ Groupes abéliens de types finis. [ROM]

Théorème 15 : Théorème de structure des groupes abéliens de type fini.

Corollaire 16 : Théorème de structure des groupes abéliens finis.

Application 17 : Détermination à isomorphismes près de tous les groupes abéliens d'ordre donné avec théorème chinois.

II/ Le cas du groupe symétrique et applications.

A/ Systèmes de générateurs. [PER] [ROM] [U] [CAL]

Théorème 18 : Théorème de décomposition en cycles disjoints des permutations.

Application 19 : Détermination de l'ordre d'une permutation.

Corollaire 20 : Les transpositions engendrent $\mathfrak{S}_n$.

Exemple 21 : Exemple de décomposition.

Application 22 : Théorème de Schwartz.

Application 23 : Groupes d'isométries du tétraèdre et du cube.

Proposition 24 : Les autres systèmes de générateurs de $\mathfrak{S}_n$ sont $\{(1,k)\}$, $\{(k,k+1)\}$ et $\{(1,2),(1,2,\dots,n)\}$.

Remarque 25 : Il est utile d'avoir des systèmes de générateurs de cardinaux petits.

B/ Cas du groupe alterné. [ROM]

Proposition 26 : Existence et unicité du morphisme signature.

Définition 27 : Groupe alterné.

Développement 1

Lemme 28 : $\mathfrak{A}_n$ est engendré par les 3-cycles et y sont conjugués.

Théorème 29 : $\mathfrak{A}_n$ est simple pour $n \geq 5$.

Corollaire 30 : Les sous-groupes distingués de $\mathfrak{S}_n$.

III/ Le cas du groupe linéaire et ses sous-groupes.

A/ Systèmes de générateurs. [ROM] [PER] [FGNAlg2]

Définition 31 : Matrices de transvections et dilatations.

Développement 2.a)

Théorème 32 : $\mathrm{SL}_n(\mathbb{K})$ est engendré par les transvections.

Corollaire 33 : $\mathrm{GL}_n(\mathbb{K})$ est engendré par les transvections et dilatations.

Corollaire 34 : Les sous-groupes dérivés.

Proposition 35 : Systèmes de générateurs de $\mathrm{O}_n(\mathbb{R})$ et $\mathrm{SO}_n(\mathbb{R})$.

Corollaire 36 : Les sous-groupes dérivés.

B/ Applications en topologie. [ROM] [FGNAlg2]

Développement 2.b)

Proposition 37 : $\mathrm{GL}_n(\mathbb{R})$ a deux composantes connexes.

Proposition 38 : $\mathrm{SL}_n(\mathbb{K})$ est connexe par arcs.

Proposition 39 : $\mathrm{O}_n(\mathbb{R})$ a deux composantes connexes : $\mathrm{SO}_n(\mathbb{R})$ et $\mathrm{O}_n^-(\mathbb{R})$.

Références :

— [PER] Perrin p. 9 et p. 95
— [ROM] Rombaldi Algèbre 2nd éd. p. 37, p. 139 et p. 279
— [U] Ulmer Théorie des groupes p. 46, p. 55-59
— [CAL] Caldéro Histoires hédonistes tome 1 p. 250
— [FGNAlg2] Francinou Gianella Nicolas Algèbre 2 p. 177

Leçon n° 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

Soit $n \geq 2$ un entier et p un premier.

I/ Construction de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

A/ Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. [ROM]

Définition 1 : Congruence mod n.

Proposition 2 : Somme et produit de congruences.

Définition 3 : Définition de $\mathbb{Z}/n\mathbb{Z}$ et groupe avec l'addition mod n.

Proposition 4 : $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n et tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Application 5 : $\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Théorème 6 : Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 7 : Théorème de structure des groupes abéliens finis.

Exemple 8 : Les groupes abéliens d'ordre 24.

B/ L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. [ROM]

Proposition 9 : $\mathbb{Z}$ est principal et ses idéaux sont les $n\mathbb{Z}$.

Corollaire 10 : Il existe une unique structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$ rendant la surjection canonique un morphisme d'anneaux.

Théorème 11 : $a \wedge n = 1 \Leftrightarrow \overline{a}$ est générateur de $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Application 12 : $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Définition 13 : Indicatrice d'Euler.

Exemple 14 : $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, $\varphi(p) = p-1$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Exemple 15 : $n = \sum_{d|n} \varphi(d)$.

Corollaire 16 : Les diviseurs de 0 dans $\mathbb{Z}/n\mathbb{Z}$ sont $\mathbb{Z}/n\mathbb{Z} \backslash ((\mathbb{Z}/n\mathbb{Z})^\times \cup \{0\})$.

Corollaire 17 : Les idéaux de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 18 : $\mathbb{Z}/n\mathbb{Z}$ intègre $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ corps $\Leftrightarrow n$ premier.

Théorème 19 : Théorème chinois général et expression explicite de l'inverse.

Application 20 : Calcul du déterminant sur $\mathbb{Z}$ informatiquement : soit $M \in \mathrm{M}_n(\mathbb{Z})$, on considère $H = \max_{i,j \in [\![1,n]\!]} |m_{i,j}|$ et prenons $p_1, \dots, p_r$ des premiers distincts tels que $p_1 \dots p_r > 2n!H^n$ (de telle sorte à ce que $\det(M) < p_1 \dots p_r$), on calcule $\det(\overline{M})$ dans $\mathbb{F}_{p_i}$ pour tout i et par le théorème chinois on a donc $\det(M)$ dans $\mathbb{Z}$.

Corollaire 21 : φ est multiplicative.

Application 22 : Avec le théorème de structure des groupes abéliens et le théorème chinois, on peut trouver à isomorphisme près tous les groupes abéliens d'ordre fini.

Théorème 23 : $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Théorème 24 : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique ssi $n = 2, 4, p^\alpha, 2p^\alpha$.

II/ Application dans différents domaines des mathématiques

A/ Test de primalité et RSA. [ROM] [G]

Théorème 25 : Euler.

Théorème 26 : Fermat.

Remarque 27 : Réciproque fausse, nombres de Carmichaël.

Application 28 : RSA.

Application 29 : Test de primalité de Fermat.

B/ Équations arithmétiques. [ROM]

Théorème 30 : Résolution de $ax \equiv b[n]$.

Application 31 : Application du théorème chinois à la résolution de systèmes de congruences.

Exemple 32 : Résolution du système de congruences $k \equiv 2[4], 3[5], 1[9]$.

C/ Application à la théorie des corps. [PER]

Proposition 33 : Caractéristique et $\mathbb{F}_p$ sous-corps premier des $\mathbb{K}$ de caractéristique p.

Corollaire 34 : Les corps finis sont de cardinalité une puissance d'un nombre premier.

Théorème 35 : Existence et unicité des corps finis.

Exemple 36 : Construction explicite de $\mathbb{F}_4 = \mathbb{Z}/2\mathbb{Z}[X]/(X^2+X+1)$.

D/ Étude des carrés de $\mathbb{Z}/p\mathbb{Z}$. [ROM]

Proposition 37 : Nombres de carrés dans $\mathbb{F}_p$.

Proposition 38 : Caractérisation des carrés.

Application 39 : Algorithme pour trouver des carrés dans $\mathbb{F}_p$.

Corollaire 40 : -1 est un carré mod $p \Leftrightarrow p \equiv 1[4]$.

Développement 1

Application 41 : Théorème des deux carrés.

Définition 42 : Symbole de Legendre.

Théorème 43 : C'est un morphisme.

Lemme 44 : Réduction des formes quadratiques sur $\mathbb{F}_p$.

Développement 2

Théorème 45 : Loi de réciprocité quadratique.

Proposition 46 : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Application 47 : On peut calculer tous les symboles de Legendre, exemple de calcul d'un d'entre eux.

Références :

— [PER] Perrin p. 72
— [ROM] Rombaldi Algèbre 2nd éd. p. 279-294 et p. 426
— [G] Gourdon Algèbre p. 34-37

Leçon n° 121 : Nombres premiers. Applications.

I/ Généralités sur les nombres premiers.

A/ Nombres premiers. [ROM]

Définition 1 : Nombre premier et ensemble $\mathcal{P}$.

Exemple 2 : 2, 3, 5, 7, 11 sont premiers mais pas $6 = 2 \times 3$.

Lemme 3 : Lemme d'Euclide : tout $x \in \mathbb{Z} \setminus \{-1, 0, 1\}$ admet un diviseur premier.

Théorème 4 : Décomposition en facteurs premiers.

Application 5 : $\mathbb{Z}$ est principal et ses idéaux maximaux sont les $p\mathbb{Z}$ avec $p \in \mathcal{P}$.

Application 6 : Calcul de pgcd et ppcm.

Exemple 7 : $18 = 2 \times 3^2$.

B/ Répartition des nombres premiers. [ROM]

Théorème 8 : $\mathcal{P}$ est de cardinal infini.

Proposition 9 : Crible d'Ératosthène.

Théorème 10 : [Culturel] Théorème de Bertrand.

Théorème 11 : [Culturel] Théorème de De La Vallée-Poussin.

II/ Tests de primalité et cryptographie RSA. [ROM] [G]

Théorème 12 : Euler.

Théorème 13 : Fermat.

Remarque 14 : Réciproque fausse, nombres de Carmichaël.

Application 15 : Test de primalité de Fermat.

Application 16 : Cryptographie RSA.

Théorème 17 : Théorème de Wilson

III/ Applications en algèbre.

A/ En théorie des groupes. [PER]

Définition 18 : p-sous-groupe de Sylow.

Théorème 19 : Théorème de Sylow 1 : Existence des p-Sylows.

Théorème 20 : Théorème de Sylow 2 : Dénombrement des p-Sylows et ils sont tous conjugués.

Corollaire 21 : Un p-Sylow est unique ssi il est distingué.

Application 22 : Un sous-groupe d'ordre 63 n'est pas simple. Les groupes d'ordre pq avec p et q premiers distincts ne sont pas simples.

B/ En théorie des corps. [PER] [ROM]

Proposition 23 : Caractéristique et $\mathbb{F}_p$ sous-corps premier des $\mathbb{K}$ de caractéristique p.

Corollaire 24 : Les corps finis sont de cardinalité une puissance d'un nombre premier.

Théorème 25 : Existence et unicité des corps finis.

Exemple 26 : Construction explicite de $\mathbb{F}_4$.

Définition 27 : Morphisme de Frobenius.

Proposition 28 : C'est un automorphisme.

Théorème 29 : L'ensemble des $\mathbb{F}_p$-isomorphismes de $\mathbb{F}_q$ est cyclique engendré par le Frobenius.

Proposition 30 : Calcul du déterminant sur $\mathbb{Z}$ informatiquement : soit $M \in \mathrm{M}_n(\mathbb{Z})$, on considère $H = \max_{i,j \in [\![1,n]\!]} |m_{i,j}|$ et prenons $p_1, \dots, p_r$ des premiers distincts tels que $p_1 \dots p_r > 2n! H^n$ (de telle sorte à ce que $\det(M) < p_1 \dots p_r$), on calcule $\det(\overline{M})$ dans $\mathbb{F}_{p_i}$ pour tout i et par le théorème chinois on a donc $\det(M)$ dans $\mathbb{Z}$.

C/ Étude des carrés dans $\mathbb{F}_p$. [PER] [ROM]

Proposition 31 : Nombres de carrés dans $\mathbb{F}_p$.

Proposition 32 : Caractérisation des carrés : x est un carré $\Longleftrightarrow x^{\frac{p-1}{2}} = 1$ et x est un non carré $\Longleftrightarrow x^{\frac{p-1}{2}} = -1$.

Application 33 : Algorithme pour trouver des carrés dans $\mathbb{F}_p$: tirer au hasard un élément de $x \in \mathbb{Z}/p\mathbb{Z}$ et calculer $x^{\frac{p-1}{2}}$ pour tester s'il s'agit d'un carré ou non.

Corollaire 34 : -1 est un carré mod $p \Leftrightarrow p = 2$ ou $p \equiv 1[4]$.

Développement 1

Application 35 : Théorème des deux carrés.

Définition 36 : Symbole de Legendre.

Théorème 37 : C'est un morphisme.

Lemme 38 : Réduction des formes quadratiques sur $\mathbb{F}_p$.

Développement 2

Théorème 39 : Loi de réciprocité quadratique.

Proposition 40 : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Application 41 : On peut calculer tous les symboles de Legendre, exemple de calcul d'un d'entre eux.

D/ Irréductibles de $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ et réduction mod p. [PER]

Proposition 42 : Eisenstein dans $\mathbb{Z}[X]$.

Application 43 : Il existe des polynômes irréductibles de tout degré dans $\mathbb{Q}[X]$ (considérer les $X^n - p$ avec p premier) et $\overline{\mathbb{Q}}$ est donc de dimension infinie en tant que $\mathbb{Q}$-espace vectoriel.

Proposition 44 : Irréductibles et réduction mod p.

Définition 45 : Polynôme cyclotomique Φ_n.

Proposition 46 : $\Phi_n \in \mathbb{Z}[X]$ unitaire.

Théorème 47 : Il sont irréductibles dans $\mathbb{Z}[X]$ et donc dans $\mathbb{Q}[X]$ car unitaires.

Corollaire 48 : $[\mathbb{Q}(e^{\frac{2i\pi}{n}}) : \mathbb{Q}] = \varphi(n)$.

Références :

— [PER] Perrin p. 18, p. 72 et p. 76
— [ROM] Rombaldi Algèbre 2nd éd. p. 303 et p. 426
— [G] Gourdon Algèbre p. 34-37

Leçon n° 122 : Anneaux principaux. Applications.

Soit A un anneau commutatif intègre.

I/ Arithmétique dans les anneaux principaux.

A/ Vocabulaire général. [ROM]

Définition 1 : Idéal et idéal principal.

Définition 2 : Divisibilité.

Définition 3 : Éléments associés.

Définition 4 : Éléments premiers et irréductibles.

Proposition 5 : Si a est premier alors a est irréductible.

Exemple 6 : Dans $\mathbb{Z}$, les nombres premiers sont premiers.

Définition 7 : PGCD et PPCM.

Remarque 8 : N'existent pas toujours.

B/ Le cas des anneaux principaux. [ROM]

Définition 9 : Anneau principal.

Exemple 10 : $\mathbb{Z}$ et $\mathbb{K}[X]$.

Lemme 11 : Irréductible $\Rightarrow$ premier et les idéaux.

Proposition 12 : $A[X]$ est principal $\Leftrightarrow$ A est un corps.

Exemple 13 : $\mathbb{Z}[X]$ n'est pas principal car l'idéal $(2, X)$ n'est pas principal et $\mathbb{Q}(\sqrt{j})[X]$ est principal.

Théorème 14 : Existence du PGCD et du PPCM dans les anneaux principaux.

Corollaire 15 : Lemme de Gauss.

Théorème 16 : Théorème chinois.

Remarque 17 : Dans le cas de $\mathbb{Z}$, avec le théorème de structure des groupes abéliens finis, on peut obtenir tous les groupes abéliens finis à isomorphisme près.

Application 18 : Calcul du déterminant sur $\mathbb{Z}$ informatiquement : soit $M \in \mathrm{M}_n(\mathbb{Z})$, on considère $H = \max_{i,j \in [\![1,n]\!]} |m_{i,j}|$ et prenons $p_1, \ldots, p_r$ des premiers distincts tels que $p_1 \ldots p_r > 2n! H^n$ (de telle sorte à ce que $\det(M) < p_1 \ldots p_r$), on calcule $\det(\overline{M})$ dans $\mathbb{F}_{p_i}$ pour tout i et par le théorème chinois on a donc $\det(M)$ dans $\mathbb{Z}$.

C/ Anneaux factoriels. [ROM]

Définition 19 : Anneau factoriel.

Théorème 20 : A factoriel $\Leftrightarrow$ toute suite d'idéaux croissante stationne et tout élément premier est irréductible.

Corollaire 21 : Les anneaux principaux sont factoriels.

Application 22 : Décomposition en nombres premiers.

Application 23 : Calcul du PGCD et du PPCM avec la décomposition.

Exemple 24 : $\mathbb{K}[X]$ est factoriel : décomposition dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

Proposition 25 : A factoriel $\implies$ $A[X]$ factoriel.

II/ Applications aux anneaux euclidiens.

A/ Généralités. [ROM] [PER]

Définition 26 : Anneau euclidien.

Proposition 27 : Euclidien $\implies$ principal.

Exemple 28 : $\mathbb{Z}$ et $\mathbb{K}[X]$.

Algorithme 29 : Algorithme d'Euclide et complexité dans $\mathbb{Z}$ et $\mathbb{K}[X]$.

Contre-exemple 30 : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ n'est pas euclidien.

B/ L'anneau des entiers de Gauss $\mathbb{Z}[i]$. [PER]

Définition 31 : Entiers de Gauss $\mathbb{Z}[i]$.

Proposition 32 : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Développement 1

Proposition 33 : $\mathbb{Z}[i]$ euclidien.

Théorème 34 : Théorème des deux carrés.

Corollaire 35 : Irréductibles de $\mathbb{Z}[i]$.

C/ Théorème des facteurs invariants dans $M_n(A)$. [OBJ]

Développement 2

Théorème 36 : Forme normale de Smith : existence et unicité.

Application 37 : Théorème de la base adaptée sur $\mathbb{Z}$.

Application 38 : Théorème de structure des groupes abéliens finis.

III/ Autres applications.

A/ Équations diophantiennes. [ROM]

Proposition 39 : Résolution de $ax + by = c$: solution ssi $a \wedge b \mid c$.

Application 40 : Résolution de systèmes de congruence dans $\mathbb{Z}$ grâce au théorème chinois.

Exemple 41 : Exemple de résolution.

B/ En algèbre linéaire. [ROM]

Définition 42 : Polynôme minimal d'une matrice.

Proposition 43 : $\dim_{\mathbb{K}}(\mathbb{K}[M]) = \deg(\pi_M)$.

Lemme 44 : Lemme des noyaux.

Théorème 45 : Décomposition de Dunford.

Références :

— [PER] Perrin p. 45-59
— [ROM] Rombaldi Algèbre 2nd éd. p. 213, p. 237 et p. 261
— [OBJ] Beck, Malick Peyré Objectif Agrégation p. 285

Leçon n°123 : Corps finis. Applications.

I/ Construction des corps finis.

A/ Prérequis sur les extensions de corps. [PER]

Définition 1 : Degré d'une extension.

Théorème 2 : Base télescopique.

Définition 3 : Corps de rupture.

Théorème 4 : Existence et unicité des corps de rupture.

Remarque 5 : Construction explicite du corps de rupture.

Définition 6 : Corps de décomposition.

Théorème 7 : Existence et unicité du corps de décomposition.

B/ Construction théorique [PER]

Définition 8 : Caractéristique et sous-corps premier.

Corollaire 9 : Si $\mathbb{K}$ est infini alors $\mathrm{car}(\mathbb{K}) = 0$.

Corollaire 10 : Tout corps fini est de cardinal la puissance d'un nombre premier.

Remarque 11 : Il n'existe donc pas de corps de cardinal 6.

Lemme 12 : Morphismes de Frobenius.

Théorème 13 : Existence et unicité des corps finis.

Théorème 14 : Théorème de Wedderburn.

C/ Construction explicite [ROM]

Développement 1

Théorème 15 : $X^{p^n} - X = \prod_{d|n} \prod_{P \in U_n(p)} P$ et dénombrement des polynômes irréductibles de degré donné avec équivalent.

Corollaire 16 : Il existe des polynômes irréductibles de tout degré, donc construction explicite de $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ où P irréductible de $\mathbb{F}_p[X]$ de degré n, plus facile à manipuler informatiquement.

Exemple 17 : Construction de $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$ et $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$.

D/ Éléments de structure. [PER] [ROM]

Proposition 18 : Inclusion des $\mathbb{F}_{p^n}$: $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \equiv n|m$.

Proposition 19 : $\mathbb{F}_q^\times$ est cyclique.

Corollaire 20 : Théorème de l'élément primitif pour les corps finis.

Remarque 21 : On retrouve le fait qu'il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_p$ en écrivant $\mathbb{F}_q = \mathbb{F}_p[a]$ et en prenant le polynôme minimal de a.

Théorème 22 : Le groupe des $\mathbb{F}_p$-automorphismes de $\mathbb{F}_q$ est cyclique engendré par le morphisme de Frobenius.

II/ Les carrés d'un corps fini. [ROM 428-431]

Proposition 23 : Nombre de carrés de $\mathbb{F}_q^\times$ et $\mathbb{F}_q$.

Proposition 24 : Critère d'Euler pour les carrés.

Corollaire 25 : Produit de deux carrés et produit d'un carré et d'un non-carré.

Corollaire 26 : $ax^2 + by^2 = c$ admet des solutions dans $(\mathbb{F}_p)^2$.

Remarque 27 : Si on prend $a = 1$ et $b = 1$, tout élément de $\mathbb{F}_q$ s'écrit comme somme de deux carrés.

Définition 28 : Symbole de Legendre.

Proposition 29 : Le symbole de Legendre est l'unique morphisme de $\mathbb{F}_p^\times$ dans $\{\pm 1\}$.

Corollaire 30 : Théorème de Frobenius-Zolotarev.

Proposition 31 : Le nombre de solutions de $ax^2 = 1$ est $1 + \left(\frac{a}{p}\right)$

Théorème 32 : Loi de réciprocité quadratique.

Proposition 33 : Calculs de $\left(\frac{-1}{p}\right)$ et $\left(\frac{2}{p}\right)$.

Remarque 34 : On peut donc calculer tous les symboles de Legendre.

Exemple 35 : Exemple du calcul de $\left(\frac{13}{31}\right) = -1$.

III/ Applications des corps finis.

A/ Sur les polynômes. [PER] [OBJ]

Théorème 36 : Critère d'Eisenstein.

Exemple 37 : Polynôme cyclotomique pour p premier et $Y - X(X-1)(X+1)$ dans $\mathbb{K}[X,Y]$.

Théorème 38 : Réduction mod p des polynômes.

Exemple 39 : $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Z}[X]$.

Théorème 40 : $P \in \mathbb{F}_p[X]$ de degré n est irréductible $\iff$ P n'a pas de racine dans les extensions de degré au plus $\frac{n}{2}$ de $\mathbb{F}_p$.

Corollaire 41 : $X^4 + 1$ réductible mod tout p mais est irréductible sur $\mathbb{Q}$ (c'est le 8ème polynôme cyclotomique).

Développement 2

Algorithme 42 : Algorithme de Berlekamp.

B/ Dénombrement et isomorphismes exceptionnels. [CAL]

Définition 43 : Définition des groupes projectifs.

Proposition 44 : L'action sur les droites est transitive.

Proposition 45 : Dénombrement des différents groupes.

Théorème 46 : Isomorphismes exceptionnels.

Références :

— [PER] Perrin p. 65-82
— [ROM] Rombaldi Algèbre 2nd éd. p. 421 et p. 425
— [OBJ] Beck, Malick Peyré Objectif Agrégation p. 244
— [CAL] Caldéro Histoires hédonistes tome 1 p. 250

Leçon n°125 : Extensions de corps. Exemples et applications.

Dans toute la suite on considérera $\mathbb{K}$, $\mathbb{L}$ et $\mathbb{M}$ trois corps.

I/ Extensions de corps.

A/ Définitions générales. [PER]

Définition 1 : Extension.

Exemple 2 : Exemples d'extensions.

Remarque 3 : Si $\mathbb{L}/\mathbb{K}$ est une extension alors $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel.

Définition 4 : Degré d'une extension.

Remarque 5 : Pour des corps finis, $|\mathbb{L}| = |\mathbb{K}|^n$.

Théorème 6 : Multiplicativité des degrés.

Définition 7 : $\mathbb{K}[\alpha]$ et $\mathbb{K}[\alpha_1, \ldots, \alpha_n]$.

B/ Éléments algébriques et transcendants. [PER]

Définition 8 : Élément algébrique, transcendant et polynôme minimal.

Exemple 9 : $T \in \mathbb{K}(T)$ est transcendant sur $\mathbb{K}$, $\sqrt{2}$, i sont algébriques.

Proposition 10 : Si α est transcendant, alors $\mathbb{K}[\alpha] \simeq \mathbb{K}[T]$ et $\mathbb{K}(\alpha) \simeq \mathbb{K}(T)$.

Théorème 11 : Équivalence pour les éléments algébriques.

Proposition 12 : Le polynôme minimal est irréductible et définit le degré d'un élément algébrique.

Exemple 13 : $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(i)$ sont des extensions de degré 2 sur $\mathbb{Q}$. Les racines primitives n-èmes de l'unité sont algébriques de degré $\varphi(n)$.

Définition 14 : Extensions finies et algébriques.

Proposition 15 : Une extension finie est algébrique.

Théorème 16 : Si $\mathbb{L}/\mathbb{K}$ est une extension, alors $\mathbb{M} = \{x \in \mathbb{L} \mid x \text{ est algébrique sur } \mathbb{K}\}$ est un sous-corps de $\mathbb{L}$.

Remarque 17 : On peut utiliser le résultant pour calculer des polynômes annulateurs de sommes ou produits de nombres algébriques.

Définition 18 : Corps algébriquement clos.

Exemple 19 : $\mathbb{C}$.

Théorème 20 : Critère d'Eisenstein.

Remarque 21 : $X^n - 2$ est irréductible sur $\mathbb{Q}$ pour tout $n \in \mathbb{N}^*$, donc $\overline{\mathbb{Q}}$ est de dimension infinie en tant que $\mathbb{Q}$-ev.

II/ Extensions et polynômes.

A/ Corps de rupture. [PER]

Définition 22 : Corps de rupture.

Théorème 23 : Existence et unicité.

Exemple 24 : Exemples de corps de rupture.

Théorème 25 : $P \in \mathbb{K}[X]$ de degré n est irréductible $\iff$ P n'a pas de racine dans les extensions de degré au plus $\frac{n}{2}$ de $\mathbb{K}$.

Corollaire 26 : $X^4 + 1$ réductible mod tout p mais est irréductible sur $\mathbb{Q}$ (c'est le 8ème polynôme cyclotomique).

B/ Corps de décomposition. [PER]

Définition 27 : Corps de décomposition.

Théorème 28 : Existence et unicité.

Exemple 29 : Exemples de corps de décomposition.

Théorème 30 : Théorème de l'élément primitif.

Remarque 31 : Le théorème de l'élément primitif est faux en général, considérer un corps infini de caractéristique non nulle.

C/ Corps finis. [PER] [ROM] [OBJ]

Définition 32 : Caractéristique et inclusion selon la caractéristique.

Remarque 33 : Un corps fini est de cardinal une puissance d'un nombre premier.

Proposition 34 : Morphismes de Frobenius.

Théorème 35 : Existence et unicité des corps finis.

Proposition 36 : $\mathbb{F}_q^\times$ est cyclique.

Remarque 37 : Ce résultat permet de démontrer le théorème de l'élément primitif dans le cas fini.

Développement 1

Notation 38 : Notation $U_n(p)$ et $I(n,p)$.

Théorème 39 : $X^{p^n} - X = \prod_{d|n} \prod_{P \in U_d(p)} P$, équivalent et $I(n,p) \geq 1$.

Corollaire 40 : Il existe des polynômes irréductibles de tout degré, donc construction explicite de $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ où P irréductible de $\mathbb{F}_p[X]$ de degré n, plus facile à manipuler informatiquement.

Exemple 41 : Construction de $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$ et $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$.

Algorithme 42 : Algorithme de Berlekamp.

III/ Nombres constructibles.

A/ Définitions et propriétés. [CAR]

Définition 43 : Points constructibles.

Proposition 44 : Construction des parallèles, médiatrices, bissectrices.

Théorème 45 : L'ensemble $\mathcal{C}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

B/ Lien avec la théorie des corps. [CAR]

Lemme 46 : Équations pour droites et cercles.

Développement 2.a)

Théorème 47 : Théorème de Wantzel.

Corollaire 48 : Résultat de Wantzel.

C/ Réponse aux trois problèmes historiques. [CAR]

Développement 2.b)

Corollaire 49 : La duplication du cube est impossible.

Corollaire 50 : La quadrature du cercle est impossible.

Corollaire 51 : La trissection de l'angle est impossible en général.

Références :

— [PER] Perrin p. 65-80
— [ROM] Rombaldi Algèbre 2nd éd. p. 415
— [CAR] Carréga Théorie des corps p. 13-37
— [OBJ] Beck, Malick Peyré Objectif Agrégation p. 244

Leçon n° 127 : Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.

I/ Rationnalité et algébricité.

A/ Rationnels et irrationnels. [DUV]

Définition 1 : Rationnel : corps de fractions de $\mathbb{Z}$, irrationnels.

Exemple 2 : Exemples : $\sqrt{2}$, $e \in \mathbb{R}\backslash\mathbb{Q}$ et exemples de rationnels.

Définition 3 : Définition de π comme le périmètre du demi-cercle unité.

Proposition 4 : π se définit de manière équivalente comme le générateur du noyau du morphisme $t \mapsto e^{2it}$.

Proposition 5 : π est irrationnel.

Proposition 6 : Si $\theta \in \mathbb{R}\backslash\mathbb{Q}$, alors $\mathbb{Z} + \theta\mathbb{Z}$ est dense dans $\mathbb{R}$.

Application 7 : Les applications continues 1 et $\sqrt{2}$ périodiques sont constantes.

B/ Algébricité, transcendance. [PER] [DUV]

Définition 8 : Algébrique et transcendant avec application.

Exemple 9 : Exemples de nombres algébriques sur $\mathbb{Q}$.

Définition 10 : Définition de $\mathbb{K}[\alpha]$ et $\mathbb{K}(\alpha)$.

Proposition 11 : α est algébrique si et seulement si $[\mathbb{K}(\alpha) : \mathbb{K}] < +\infty$.

Théorème 12 : $\mathbb{M} = \{x \in \mathbb{L} \mid x \text{ est algébrique sur } \mathbb{K}\}$ est un sous-corps.

Application 13 : $\overline{\mathbb{Q}}$ est un sous-corps de $\mathbb{C}$.

Remarque 14 : Avec les résultants, on peut trouver un polynôme annulateur de la somme ou du produit d'éléments algébriques.

Théorème 15 : (admis) π et e sont transcendants.

Théorème 16 : Condition vérifiée par les algébriques.

Définition 17 : Nombres de Liouville.

Proposition 18 : Les nombres de Liouville sont transcendants.

Application 19 : $\sum_{k=0}^{+\infty} \frac{1}{10^{k!}}$ est transcendant.

II/ Anneaux $\mathbb{Z}[\omega]$ et application en arithmétique.

A/ Généralités. [DUV] [PER]

Proposition 20 : $\mathbb{Q}(\sqrt{d})$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ avec pour $\mathbb{Q}$-base $(1, \sqrt{d})$.

Proposition 21 : Les anneaux des entiers de $\mathbb{Q}(\sqrt{d})$ sont les $\mathbb{Z}[\omega]$, ω variant selon la congruence de d.

Exemple 22 : Les entiers de Gauss $\mathbb{Z}[i]$ et les entiers d'Eisenstein $\mathbb{Z}[j]$.

Proposition 23 : Les inversibles de $\mathbb{Z}[\omega]$.

Application 24 : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ et $\mathbb{Z}[j]^\times = \{\pm 1, \pm 1 \pm j\}$.

Théorème 25 : Valeurs de d pour lesquelles $\mathbb{Z}[\omega]$ est euclidien.

Contre-exemple 26 : $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel $(6 = 3 \times 2 = (1 + i\sqrt{5})(1 - i\sqrt{5}))$ donc n'est pas euclidien.

B/ Théorème des deux carrés de Fermat. [PER]

Définition 27 : Ensemble Σ.

Proposition 28 : Σ est stable par produit.

Développement 1

$p \in \Sigma \Leftrightarrow p = 2 \text{ ou } p \equiv 1 \mod 4.$

Théorème 29 : $n \in \Sigma \iff v_p(n)$ pair pour tout $p \equiv 3[4]$

Proposition 30 : Irréductibles de $\mathbb{Z}[i]$.

C/ Application : résolution d'équations diophantiennes. [DUV]

Application 31 : Résolution de l'équation de Mordell $y^2 = x^3 - 11$.

Application 32 : Résolution de $x^5 - y^2 = 1$.

III/ Construction à la règle et au compas.

A/ Définitions et propriétés. [CAR]

Définition 33 : Points constructibles.

Proposition 34 : Construction des parallèles, médiatrices, bissectrices.

Théorème 35 : L'ensemble $\mathcal{C}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

B/ Lien avec la théorie des corps. [CAR]

Lemme 36 : Équations pour droites et cercles.

Développement 2.a)

Théorème 37 : Théorème de Wantzel.

Corollaire 38 : Résultat de Wantzel.

C/ Réponse aux trois problèmes historiques. [CAR]

Développement 2.b)

Corollaire 39 : La duplication du cube est impossible.

Corollaire 40 : La quadrature du cercle est impossible.

Corollaire 41 : La trissection de l'angle est impossible en général.

Références :

— [PER] Perrin p. 65-68 et p. 56

— [DUV] Duverney Théorie des nombres p. 1, p. 47 et p. 110

— [CAR] Carréga Théorie des corps p. 13-37

Leçon n°141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Soit $\mathbb{K}$ un corps et A un anneau commutatif intègre.

I/ Irréductibilité dans $A[X]$

A/ Définition et premières propriétés. [PER]

Définition 1 : Définition de polynôme irréductible.

Remarque 2 : $A[X]^{\times} = A^{\times}$.

Exemple 3 : $2X$ est réductible dans $\mathbb{Z}[X]$ mais irréductible dans $\mathbb{R}[X]$.

Proposition 4 : Si $P \in \mathbb{K}[X]$ est irréductible et $\deg(P) > 1$ alors P n'a pas de racine dans $\mathbb{K}$.

Exemple 5 : Pour tout $a \in \mathbb{K}$, $X - a$ est irréductible dans $\mathbb{K}[X]$.

Contre-exemple 6 : La réciproque est fausse : $(X^2+1)^2$ dans $\mathbb{R}[X]$.

Proposition 7 : Les polynômes de degré 2 ou 3 sans racine dans $\mathbb{K}$ sont irréductibles.

Exemple 8 : Les polynômes irréductibles dans $\mathbb{R}[X]$.

Proposition 9 : $\mathbb{K}[X]$ est un anneau euclidien.

Proposition 10 : Division dans $A[X]$ avec coefficient dominant inversible.

Théorème 11 : Si A est factoriel alors $A[X]$ est factoriel.

Définition 12 : Contenu d'un polynôme.

Proposition 13 : $c(PQ) = c(P)c(Q)$.

Proposition 14 : Les irréductibles de $A[X]$ en fonction de ceux de $\mathrm{Frac}(A)[X]$.

B/ Premiers critères d'irréductibilité. [PER]

Théorème 15 : Critère d'Eisenstein.

Exemple 16 : Le p-ième polynôme cyclotomique et $Y^2 - X(X-1)(X-2)$ dans $\mathbb{R}[X]$, $X^n - 2$ est irréductible sur $\mathbb{Q}$ pour tout $n \in \mathbb{N}^*$ et donc $\overline{\mathbb{Q}}$ est de dimension infinie en tant que $\mathbb{Q}$-ev.

Théorème 17 : Réduction modulo un idéal.

Exemple 18 : $X^3+462X^2+2433X-67691$ est irréductible dans $\mathbb{Z}[X]$, X^2+Y^2+1 est irréductible dans $\mathbb{R}[X,Y]$.

II/ Théorie des corps et irréductibilité.

A/ Prérequis de la théorie des corps. [PER]

Définition 19 : Extension de corps.

Définition 20 : Degré d'une extension.

Théorème 21 : Multiplicativité des degrés d'extension.

Définition 22 : $\mathbb{K}[\alpha]$ et $\mathbb{K}(\alpha)$.

Exemple 23 : $\sqrt{2}$, i, $2^{\frac{1}{3}}$ sont algébriques et T est transcendant dans $\mathbb{K}(T)$.

Théorème 24 : Équivalences pour être algébrique et un polynôme minimal est irréductible.

Définition 25 : Corps de rupture.

Théorème 26 : Existence et unicité des corps de rupture.

Exemple 27 : Exemples de corps de rupture.

Théorème 28 : Existence et unicité des corps de décomposition.

B/ Corps finis. [PER] [ROM] [OBJ]

Définition 29 : Caractéristique d'un corps + $\mathbb{F}_p \subset \mathbb{K}$ si $\mathrm{car}(\mathbb{K}) = p > 0$.

Théorème 30 : Existence et unicité des corps finis.

Développement 1

Théorème 31 : $X^{p^n} - X = \prod_{d|n} \prod_{P \in U_n(p)} P$ et dénombrement des polynômes irréductibles de degré donné avec équivalent.

Corollaire 32 : Il existe des polynômes irréductibles de tout degré, donc construction explicite de $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ où P irréductible de $\mathbb{F}_p[X]$ de degré n, plus facile à manipuler informatiquement.

Exemple 33 : Construction de $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$ et $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$.

Algorithme 34 : Algorithme de Berlekamp.

C/ Application à l'irréductibilité. [PER]

Théorème 35 : $P \in \mathbb{K}[X]$ de degré n est irréductible $\iff$ P n'a pas de racine dans les extensions de degré au plus $\frac{n}{2}$ de $\mathbb{K}$.

Corollaire 36 : X^4+1 réductible mod tout p mais est irréductible sur $\mathbb{Q}$ (c'est le 8ème polynôme cyclotomique).

Proposition 37 : Si un polynôme P de degré n est irréductible dans $\mathbb{K}$ et si $\mathbb{L}$ est une extension de degré m premier avec n, alors P est irréductible dans $\mathbb{L}[X]$.

III/ Cyclotomie. [PER]

Définition 38 : Racines primitives n-ièmes de l'unité.

Définition 39 : Polynômes cyclotomiques.

Proposition 40 : $X^n - 1 = \prod_{d|n} \Phi_d(X)$ et $\Phi_d(X)$ est unitaire dans $\mathbb{Z}[X]$.

Développement 2

Théorème 41 : $\Phi_n(X)$ est irréductible dans $\mathbb{Z}[X]$.

Corollaire 42 : Si $\zeta = e^{\frac{2i\pi}{n}}$, alors son polynôme minimal est Φ_n et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Corollaire 43 : Si $\mathbb{K}$ est une extension finie de $\mathbb{Q}$, alors il existe un nombre fini de racines de l'unité dans $\mathbb{K}$.

Références :

— [PER] Perrin p. p. 65-84

— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 421

— [OBJ] Beck, Malick Peyré Objectif Agrégation p. 244

Leçon n° 142 : PGCD et PPCM, algorithmes de calcul. Applications.

Soit A un anneau commutatif intègre.

I/ Notion de PGCD et PPCM dans différents types d'anneaux.

A/ Premières définitions et cas des anneaux factoriels. [ROM]

Définition 1 : Définition du PGCD et du PPCM, commutativité et associativité.

Remarque 2 : Les PGCD et PPCM sont uniques à association près.

Proposition 3 : $ab = (a \wedge b)(a \vee b)$.

Remarque 4 : Connaître le PGCD, c'est connaître le PPCM.

Exemple 5 : $(1-i \wedge 2+i) = 1-i$ dans $\mathbb{Z}[i]$, $2 \wedge 3 = 1$ dans $\mathbb{Z}$.

Proposition 6 : Existence des PGCD et PPCM dans les anneaux factoriels et expression.

Corollaire 7 : Homogénéité du PGCD et du PPCM.

Définition 8 : Premiers entre eux dans leur ensemble.

Proposition 9 : Lemme de Gauss.

Définition 10 : Le PGCD dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$.

B/ Situation dans les anneaux principaux. [ROM]

Proposition 11 : Les anneaux principaux sont factoriels donc existence du PGCD et du PPCM.

Proposition 12 : Expression en termes d'idéaux.

Corollaire 13 : Si δ est le PGCD de $a_1, \dots, a_r$, alors il existe $u_1, \dots, u_r$ tels que $\sum_{i=1}^{r} u_i a_i = \delta$.

Théorème 14 : Théorème de Bézout.

Remarque 15 : Réciproque fausse : par exemple $3(2) + 2(-2) = 2$ et $2 \wedge 3 = 1$.

Application 16 : Résolution d'équations diophantiennes $ax + by = c$.

Application 17 : Lemme des noyaux.

Corollaire 18 : Si $a \wedge c = 1$, alors $a \wedge b = a \wedge (bc)$.

Théorème 19 : Théorème des restes chinois et expression réciproque.

Application 20 : Systèmes de congruence sur $\mathbb{Z}$.

Application 21 : Calcul du déterminant sur $\mathbb{Z}$ informatiquement : soit $M \in \mathrm{M}_n(\mathbb{Z})$, on considère $H = \max\limits_{i,j \in [\![1,n]\!]} |m_{i,j}|$ et prenons $p_1, \dots, p_r$ des premiers distincts tels que $p_1 \dots p_r > 2n! H^n$ (de telle sorte à ce que $\det(M) < p_1 \dots p_r$), on calcule $\det(\overline{M})$ dans $\mathbb{F}_{p_i}$ pour tout i et par le théorème chinois on a donc $\det(M)$ dans $\mathbb{Z}$.

Application 22 : Le polynôme interpolateur de Lagrange est solution du système de congruence $P \equiv y_i \mod (X - x_i)$.

Proposition 23 : $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/(n \wedge m)\mathbb{Z} \times \mathbb{Z}/(n \vee m)\mathbb{Z}$.

II/ Cas des anneaux euclidiens : algorithmes de calcul.

A/ Algorithme d'Euclide. [ROM] [DEM]

Lemme 24 : Lemme d'Euclide.

Algorithme 25 : Algorithme d'Euclide dans les anneaux euclidiens.

Application 26 : $X^{p^n} - X \wedge X^{p^m} - X = X^{p^{n \wedge m}} - X$.

Algorithme 27 : Algorithme d'Euclide étendu.

Application 28 : Inverse dans les corps de rupture.

Algorithme 29 : Algorithme binaire.

B/ Coût de l'algorithme dans $\mathbb{Z}$ et $\mathbb{K}[X]$. [DEM]

Proposition 30 : Théorème de Lamé.

Corollaire 31 : L'algorithme d'Euclide étendu pour deux éléments a et b dans $\mathbb{Z}$ nécessite $O(\min(\log(a), \log(b)))$ opérations dans $\mathbb{Z}$.

Proposition 32 : L'algorithme d'Euclide étendu pour deux polynômes A et B nécessite $O((\deg(A)+1)(\deg(B)+1))$ opérations dans $\mathbb{K}$.

III/ Applications à d'autres domaines des mathématiques.

A/ Facteurs invariants. [OBJ]

Développement 1

Proposition 33 : Forme normale de Smith : existence et unicité.

Application 34 : Base adaptée.

Application 35 : Théorème de structure des groupes abéliens finis.

B/ Factorisation des polynômes sur un corps fini. [OBJ]

Développement 2

Algorithme 36 : Algorithme de Berlekamp.

Références :

— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 224 et p. 237-251

— [OBJ] Beck, Malick Peyré Objectif Agrégation p. 244 et p. 285

— [DEM] Demazure Cours d'Algèbre p. 33-42

Leçon n° 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et application.

Soit $\mathbb{K}$ un corps.

I/ Racines d'un polynôme.

A/ Premières propriétés. [G] [ROM]

Définition 1 : Racine d'un polynôme.

Proposition 2 : α est une racine de P ssi $X-\alpha$ divise P dans $\mathbb{K}[X]$.

Exemple 3 : Les polynômes de degré impair réels ont une racine réelle.

Définition 4 : Multiplicité d'une racine.

Proposition 5 : Expression des polynômes en fonction de leurs racines et de leurs multiplicités.

Corollaire 6 : Un polynôme de degré n sur un corps a au plus n racines.

Contre-exemple 7 : Faux si $\mathbb{K}$ n'est pas un corps : par exemple, regarder $4X$ dans $\mathbb{Z}/8\mathbb{Z}[X]$.

Proposition 8 : Si $\mathbb{K}$ est infini alors si $P \in \mathbb{K}[X]$ est tel que pour tout $x \in \mathbb{K}$, $P(x)=0$, $P=0$.

Corollaire 9 : Identification entre un polynôme et sa fonction polynomiale associée si $\mathbb{K}$ est infini.

Proposition 10 : Formule de Taylor pour les polynômes.

Corollaire 11 : Relation entre la dérivée et la multiplicité d'une racine.

Définition 12 : Polynôme scindé.

Théorème 13 : Théorème d'Alembert-Gauss.

Application 14 : Toutes les matrices complexes sont trigonalisables.

B/ Relations coefficients-racines. [G] [FGNAlg2] [ROM]

Définition 15 : Polynômes symétriques élémentaires.

Théorème 16 : Relation entre les coefficients et les racines d'un polynôme.

Proposition 17 : Formules de Newton.

Application 18 : Algorithme de Faddeev-Le Verrier.

Théorème 19 : Théorème de structure des polynômes symétriques.

Exemple 20 : $P = X^2+Y^2+Z^2 = (X+Y+Z)^2-2(XY+XZ+YZ)$.

II/ Localisation des racines d'un polynôme.

A/ Premiers résultats. [FGNAlg1]

Développement 1

Théorème 21 : Théorème de Gauss-Lucas.

Théorème 22 : Énoncé équivalent.

Application 23 : Application de Gauss-Lucas à un polynôme.

Théorème 24 : Théorème de Kronecker.

Corollaire 25 : Soit $P \in Z[X]$ unitaire de degré n et irréductible sur $\mathbb{Q}$. Si toutes les racines de P sont de module inférieur ou égal à 1, alors $P=X$ ou $P=\Phi_n$.

B/ Disques de Gershgörin. [FGNAlg2]

Définition 26 : Matrice compagnon.

Proposition 27 : Si C_P est une matrice compagnon alors $\chi_{C_p}=P$.

Proposition 28 : Disques de Gershgörin.

Remarque 29 : On applique les disques de Gershgörin sur les matrices compagnons pour localiser les racines d'un polynôme.

Proposition 30 : Si un disque est isolé, alors il y a une unique racine du polynôme dans ce disque.

C/ Approximation de racines. [PGCD]

Proposition 31 : Méthode de Newton.

Application 32 : Méthode de Héron.

Remarque 33 : On utilise la méthode de Newton après dichotomie pour s'approcher des racines (condition initiale proche de la racine)

III/ Racines de polynôme et extensions de corps.

A/ Éléments algébriques. [PER]

Définition 34 : Élément algébrique et transcendant.

Exemple 35 : $\sqrt{2}$, i et j sont algébriques sur $\mathbb{Q}$.

Proposition 36 : Un élément α est algèbrique ssi $[\mathbb{K}(\alpha) : \mathbb{K}] < +\infty$ et définition du degré d'un algébrique.

B/ Corps de rupture, décomposition, corps finis. [PER] [ROM]

Définition 37 : Corps de rupture.

Théorème 38 : Existence et unicité.

Définition 39 : Corps de décomposition.

Théorème 40 : Existence et unicité.

Théorème 41 : Existence et unicité des corps finis.

Développement 2

Théorème 42 : $X^{p^n} - X = \prod_{d|n} \prod_{P \in U_n(p)} P$ et dénombrement des polynômes irréductibles de degré donné avec équivalent.

Corollaire 43 : Il existe des polynômes irréductibles de tout degré, donc construction explicite de $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ où P irréductible de $\mathbb{F}_p[X]$ de degré n, plus facile à manipuler informatiquement.

Exemple 44 : Construction de $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$ et $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2 + 1)$.

Références :

— [PER] Perrin p. 65-73
— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 362 et p. 421
— [PGCD] Rouvière Petit guide du calcul différentiel p. 142
— [G] Gourdon Algèbre p. 53-80
— [FGNAlg1] Francinou, Gianella Nicolas Algèbre 1 p. 213 et p. 229
— [FGNAlg2] Francinou, Gianella Nicolas Algèbre 2 p. 79 et p. 80

Leçon n° 148 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

Soit $\mathbb{K}$ un corps et E un $\mathbb{K}$-espace vectoriel.

I/ Espaces vectoriels et dimension.

A/ Familles libres, génératrices, bases. [G]

Définition 1 : Famille libre, génératrice, base.

Proposition 2 : Dans un espace vectoriel E avec une $\mathbb{K}$-base $(e_i)_{i\in I}$, tout élément $x \in E$ s'écrit comme une combinaison linéaire finie d'éléments de $(e_i)_{i\in I}$.

Exemple 3 : Exemples de bases : base canonique de $\mathbb{K}^n$, base de $\mathbb{K}[X]$, base de $\mathrm{M}_n(\mathbb{K})$.

Définition 4 : Dimension finie et infinie.

Proposition 5 : Si F sev de E et E est de dimension finie, alors F est également de dimension finie.

Exemple 6 : $\mathbb{K}[X]$ est de dimension infinie et $\mathrm{S}_n(\mathbb{K})$ est de dimension finie.

B/ Théorie de la dimension. [G]

Théorème 7 : Si E est de dimension finie et $\mathcal{L}$ est une famille libre et $\mathcal{G}$ une famille génératrice, alors il existe une base $\mathcal{B}$ telle que $\mathcal{L} \subset \mathcal{B} \subset \mathcal{G}$.

Corollaire 8 : Tout espace vectoriel de dimension finie admet une base.

Corollaire 9 : Théorème de la base extraite.

Corollaire 10 : Théorème de la base incomplète.

Théorème 11 : Toutes les bases ont le même cardinal, donc $\dim(E)$ est bien défini.

Proposition 12 : Tout système libre/générateur de n vecteurs dans un espace de dimension n est une base.

Proposition 13 : Théorème de Grassmann.

Application 14 : Si $(H_i)_{i\in[\![1,p]\!]}$ p hyperplans alors $\dim\left(\bigcap_{i=1}^{p} H_i\right) \geq n-p$.

II/ Applications linéaires et rang.

A/ Applications linéaires et rang. [G]

Définition 15 : Rang d'un endomorphisme.

Théorème 16 : Théorème du rang.

Corollaire 17 : Une application linéaire f est bijective si et seulement si elle est injective si et seulement si elle est surjective.

Contre-exemple 18 : Ceci est faux en dimension infinie, par exemple avec l'application dérivation $P \mapsto P'$ sur $\mathbb{R}[X]$.

Application 19 : Le polynôme interpolateur de Lagrange : l'application $P \mapsto (P(x_1), \dots, P(x_n))$ est injective en dimension finie donc bijective.

B/ Représentation matricielle et rang d'une matrice. [G]

Proposition 20 : $\dim(\mathrm{M}_{n,p}(\mathbb{K})) = \dim(\mathcal{L}(E,F)) = np$.

Définition 21 : Matrice dans une base d'un endomorphisme et le rang est indépendant du choix de la base.

Théorème 22 : Si $\mathrm{rg}(A) = r$, alors A est équivalente à $J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

Corollaire 23 : Deux matrices sont équivalentes ssi elles ont le même rang.

Théorème 24 : Le rang d'une matrice est égal à la taille du plus grand mineur non nul de la matrice.

Application 25 : Le rang ne dépend pas de l'extension de corps.

Application 26 : La méthode du pivot de Gauss permet de déterminer le rang d'une matrice en $O(n^3)$.

III/ Applications de la dimension finie.

A/ En topologie pour les espaces vectoriels normés. [G]

Théorème 27 : Équivalence des normes.

Corollaire 28 : En dimension finie, les compacts sont les fermés bornés.

Application 29 : Toute application linéaire d'un espace vectoriel normé de dimension finie vers n'importe quel espace normé est continue.

Corollaire 30 : Tout sous-espace vectoriel de dimension finie est fermé.

Application 31 : $\exp(A) \in \mathbb{K}[A]$ pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Théorème 32 : Théorème de Riesz.

B/ Théorie de la réduction. [ROM]

Définition 33 : Endomorphismes trigonalisables.

Proposition 34 : Un endomorphisme est trigonalisable si et seulement si son polynôme caractéristique est scindé.

Exemple 35 : $\mathbb{C}$ est algébriquement clos donc tous les endomorphismes y sont trigonalisables.

Développement 1

Théorème 36 : Réduction de Jordan par la dualité.

Théorème 37 : Réduction des endomorphismes normaux.

C/ En théorie des corps. [PER]

Théorème 38 : Multiplicativité des degrés et bases télescopique.

Définition 39 : Éléments algébriques et transcendants.

Exemple 40 : Exemple d'éléments algébriques.

Proposition 41 : Un élément α est algèbrique ssi $[\mathbb{K}(\alpha) : \mathbb{K}] < +\infty$.

Théorème 42 : Existence et unicité des corps finis.

Développement 2

Algorithme 43 : Algorithme de Berlekamp.

Références :

— [PER] Perrin p. 65-73
— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 675, p. 681 et p. 745
— [G] Gourdon Algèbre p. 109-126
— [G] Gourdon Analyse p. 47-56
— [OBJ] Beck, Malick Peyré Objectif Agrégation p. 244

Leçon n° 149 : Déterminant. Exemples et applications.

Soit $\mathbb{K}$ un corps et E un $\mathbb{K}$-espace vectoriel de dimension $n \geq 1$.

I/ Notions de déterminant.

A/ Des formes multilinéaires au déterminant. [G]

Définition 1 : Forme p-linéaire et espace $\mathcal{L}_p(E,\mathbb{K})$.

Définition 2 : Formes alternées ($\mathcal{A}_p(E,\mathbb{K})$) et antisymétriques.

Théorème 3 : En $\mathrm{car}(\mathbb{K}) \neq 2$, une forme est antisymétrique si et seulement si elle est alternée.

Corollaire 4 : Si $(x_1,\ldots,x_p)$ est une famille liée, alors $f(x_1,\ldots,x_p) = 0$.

Théorème 5 : $\dim(\mathcal{A}_n(E,\mathbb{K})) = 1$, on définit le déterminant d'une base et l'expression du déterminant pour une famille de vecteurs quelconque.

Proposition 6 : Changement de base.

Théorème 7 : Une famille est liée si et seulement si son déterminant est nul.

B/ Déterminant d'une matrice carrée, d'un endomorphisme. [G]

Définition 8 : Définition du déterminant d'une matrice.

Proposition 9 : Propriétés du déterminant d'une matrice.

Définition 10 : Définition du déterminant d'un endomorphisme indépendant du choix de la base.

Remarque 11 : Lien entre le déterminant d'un endomorphisme et d'une matrice : $\det(f) = \det(\mathrm{Mat}_{\mathcal{B}}(f))$.

Remarque 12 : On peut définir le déterminant dans un anneau intègre quelconque en passant dans le corps de fractions.

C/ Propriétés analytiques et topologiques. [PGCD] [G]

Proposition 13 : Le déterminant est une application polynomiale donc C^∞.

Corollaire 14 : $\mathrm{GL}_n(\mathbb{K})$ est ouvert et $\mathrm{SL}_n(\mathbb{K})$ est fermé.

Développement 1

Proposition 15 : Différentielle du déterminant sur $\mathrm{M}_n(\mathbb{R})$: $d_M(\det)(H) = \mathrm{Tr}({}^t\mathrm{Com}(M)H)$.

Application 16 : Les éléments de $\mathrm{SO}_n(\mathbb{R})$ sont les éléments de $\mathrm{SL}_n(\mathbb{R})$ de norme 2 minimale.

II/ Méthodes de calcul du déterminant.

A/ Mineurs, cofacteurs. [G]

Définition 17 : Mineurs.

Proposition 18 : Développement par rapport à une ligne ou une colonne.

Définition 19 : Commatrice.

Proposition 20 : Relation : $A^t\mathrm{Com}(A) = \det(A)I_n$.

Corollaire 21 : Si A est inversible, alors $A^{-1} = \frac{1}{\det(A)}{}^t\mathrm{Com}(A)$.

Application 22 : $A \mapsto A^{-1}$ est continue. (fraction rationnelle en les coefficients)

B/ Cas simple, pivot de Gauss. [G] [OBJ]

Exemple 23 : Cas des matrices de taille 2 et 3 (règle de Sarrus).

Proposition 24 : Matrices triangulaires par blocs.

Corollaire 25 : Les matrices triangulaires.

Application 26 : Pivot de Gauss et complexité du calcul du déterminant dans un corps.

Application 27 : Calcul du déterminant sur $\mathbb{Z}$ informatiquement : soit $M \in \mathrm{M}_n(\mathbb{Z})$, on considère $H = \max_{i,j \in [\![1,n]\!]} |m_{i,j}|$ et prenons $p_1, \ldots, p_r$ des premiers distincts tels que $p_1 \ldots p_r > 2n!H^n$ (de telle sorte à ce que $\det(M) < p_1 \ldots p_r$), on calcule $\det(\overline{M})$ dans $\mathbb{F}_{p_i}$ pour tout i et par le théorème chinois on a donc $\det(M)$ dans $\mathbb{Z}$.

Exemple 28 : Exemple de calcul de déterminant de matrice en utilisant le pivot de Gauss :

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

C/ Déterminants remarquables. [G]

Exemple 29 : Déterminant de Vandermonde.

Développement 2

Exemple 30 : Déterminant circulant.

Application 31 : Suite de polygones.

III/ Applications à d'autres domaines des mathématiques.

A/ Interprétation géométrique du déterminant. [OBJ] [FGNAlg3]

Théorème 32 : Volume et déterminant dans $\mathbb{R}^n$.

Application 33 : Volume d'un parallélépipède.

Application 34 : Volume maximal via l'inégalité de Hadamard.

Proposition 35 : Déterminant de Gram et distance à un sev.

Théorème 36 : Théorème de changement de variable.

Lemme 37 : log-convexité du déterminant sur $S_n^{++}(\mathbb{R})$.

Application 38 : Ellipsoïde de John-Loewner.

B/ Résultant. [ROM] [SP]

Définition 39 : Résultant.

Théorème 40 : A et B sont premiers entre eux si et seulement si $\mathrm{Res}(A, B) \neq 0$.

Application 41 : Si $\mathbb{K}$ est un corps et $\mathbb{L}$ une extension, $\mathbb{M} = \{x \in \mathbb{L},\ x$ algébrique sur $\mathbb{K}\}$ est un sous-corps de $\mathbb{L}$.

Application 42 : L'ensemble $D'_n(\mathbb{C})$ des matrices diagonalisables admettant n valeurs propres distinctes est ouvert.

Application 43 : Paramétrisation rationnelle du cercle.

C/ En algèbre linéaire. [ROM]

Définition 44 : Polynôme caractéristique.

Application 45 : Les valeurs propres sont les racines, $A \mapsto \chi_A$ est continue, et l'ensemble des matrices nilpotentes est fermé.

Références :

— [OBJ] Beck, Malick Peyré Objectif Agrégation p.9 et p. 181-184
— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 581, p. 604
— [FGNAlg3] Francinou, Gianella Nicolas Algèbre 3 p. 222 et p. 229
— [SP] Saux-Picart Cours de calcul formel tome 1 p. 143-150
— [G] Gourdon Algèbre p. 134-139
— [G] Gourdon Analyse p. 321
— [PGCD] Rouvière Petit Guide du Calcul Différentiel p. 76

Leçon n° 150 : Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$.

I/ Polynômes d'endomorphismes.

A/ L'algèbre $\mathbb{K}[u]$. [MAN] [ROM]

Définition 1 : Définition de $P(u)$.

Proposition 2 : $\mathbb{K}[X] \to \mathcal{L}(E) : P \mapsto P(u)$ est un morphisme d'algèbres dont l'image est $\mathbb{K}[u]$.

Définition 3 : Polynôme minimal et idéal annulateur, qui existent toujours car $\mathcal{L}(E)$ est de dimension finie.

Proposition 4 : $\dim(\mathbb{K}[u]) = \deg(\pi_u)$.

Exemple 5 : Le polynôme minimal d'une symétrie vectorielle qui n'est pas une homothétie est $X^2 - 1$.

Remarque 6 : Polynôme minimal d'une matrice, lien avec celui des endomorphismes.

Proposition 7 : $P \in \mathbb{K}[X]$, $P(u) \in \mathbb{K}[u]^\times \iff P \wedge \pi_u = 1$.

Proposition 8 : $\mathbb{K}[u]$ est un corps si et seulement si $\mathbb{K}[u]$ est intègre, ce qui équivaut à π_u irréductible.

B/ Polynôme caractéristique. [G] [ROM] [MAN] [FGNAlg2]

Définition 9 : Polynôme caractéristique.

Proposition 10 : Si A et B sont semblables, alors $\chi_A = \chi_B$.

Corollaire 11 : On peut donc définir χ_u pour $u \in \mathcal{L}(E)$.

Exemple 12 : Cas de la dimension 2.

Algorithme 13 : Algorithme de Fadeev-LeVerrier pour le calcul du polynôme caractéristique (sommes de Newton pour exprimer les coefficients du polynôme caractéristique).

Proposition 14 : λ est valeur propre si et seulement si $\chi_u(\lambda) = 0$.

Application 15 : Matrice compagnon C_P, ses valeurs propres sont les racines de P.

Proposition 16 : $\chi_{AB} = \chi_{BA}$ pour tout $A, B \in \mathrm{M}_n(\mathbb{C})$.

Proposition 17 : La fonction $M \mapsto \chi_M$ est continue, mais pas $M \mapsto \pi_M$ pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Application 18 : L'ensemble des matrices nilpotentes est fermé pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

C/ Polynômes d'endomorphismes et sous-espaces stables. [MAN] [ROM]

Théorème 19 : Lemme des noyaux.

Application 20 : Cas où $\pi_u = \prod P_i^{\alpha_i}$.

Proposition 21 : Si F est u-stable, alors $\chi_{u|_F} | \chi_u$ et il en est de même pour le polynôme minimal.

II/ Application à la réduction des endomorphismes.

A/ Diagonalisation et trigonalisation. [BER] [ROM]

Définition 22 : Endomorphismes diagonalisables.

Proposition 23 : Critères pratiques de diagonalisation.

Proposition 24 : Critères basés sur les polynômes d'endomorphismes.

Application 25 : Une matrice est diagonalisable sur $\mathbb{F}_p$ si et seulement si $X^p - X$ l'annule.

Définition 26 : Endomorphismes trigonalisables.

Proposition 27 : u est trigonalisable si et seulement si χ_u est scindé.

Exemple 28 : Dans $\mathbb{C}$ algébriquement clos, tous les endomorphismes sont trigonalisables.

Développement 1

Théorème 29 : Décomposition de Dunford par la méthode de Newton.

B/ Réduction en sous-espaces stables. [ROM]

Théorème 30 : Réduction de Jordan.

Remarque 31 : Permet d'obtenir la matrice dans une forme privilégiée.

III/ Applications des polynômes d'endomorphismes.

A/ Calcul d'inverse et puissances. [MAN]

Proposition 32 : Si A est annulée par un polynôme $P \in \mathbb{K}[X]$ tel que $P(0) \neq 0$, alors $A^{-1} \in \mathbb{K}[A]$ et on peut exprimer l'inverse.

Application 33 : Lorsque l'on connaît un polynôme annulateur P de u, on peut calculer u^k en effectuant la division euclidienne de X^k par P.

Exemple 34 : Cas de la dimension 2 dans tous les cas.

B/ Exponentielle de matrices. [ROM] [ZAV]

On suppose ici $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Définition 35 : Exponentielle matricielle.

Proposition 36 : $e^A \in \mathrm{GL}_n(\mathbb{K})$ et $(e^A)^{-1} = e^{-A}$.

Application 37 : Calcul de l'exponentielle matricielle avec décomposition de Dunford.

Application 38 : Résolution du système différentiel $Y' = AY$.

Développement 2

Proposition 39 : $\exp(A) \in \mathbb{K}[A]$.

Lemme 40 : $\mathbb{C}[A]^\times$ est connexe par arcs.

Proposition 41 : $\exp : \mathrm{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective.

Application 42 : $\exp(\mathrm{M}_n(\mathbb{R})) = \{M^2,\ M \in \mathrm{GL}_n(\mathbb{R})\}$.

Références :

— [G] Gourdon Algèbre p. 174
— [MAN] Mansuy p. 1-48, p. 11
— [BER] Berhuy Algèbre le grand combat p. 972
— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 603 et p. 643 et p. 675
— [ZAV] Zavidovique Un max de maths p. 48
— [FGNAlg2] Francinou, Gianella Nicolas Algèbre 2 p. 79

Leçon n° 151 : Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.

Soit E un $\mathbb{K}$-ev de dimension $n \geq 1$. Soit $u \in \mathcal{L}(E)$, χ_u son polynôme caractéristique, π_u son polynôme minimal, F sous-espace vectoriel de E de dimension p.

I/ Notion de sous-espace stable.

A/ Définitions et propriétés. [OBJ] [G]

Définition 1 : F est stable par u si $u(F) \subset F$.

Exemple 2 : $\mathrm{Ker}(u)$ et $\mathrm{Im}(u)$ sont stables par u.

Exemple 3 : Si $\mathbb{K} = \mathbb{R}$, u admet une droite ou un plan stable.

Exemple 4 : u est une homothétie si et seulement si u stabilise toute droite.

Proposition 5 : Si F est stable par u alors $u|_F \in \mathcal{L}(F)$.

Proposition 6 : Caractérisation matricielle des sous-espaces vectoriels stables.

Application 7 : χ_u est irréductible si et seulement si u n'admet pas de sous-espace stable non trivial.

Application 8 : Cayley-Hamilton.

B/ Production de sous-espaces stables. [OBJ] [ROM]

Remarque 9 : Trouver des sous-espaces stables permet de trouver des formes privilégiées pour les matrices.

Proposition 10 : Si u et v commutent alors $\mathrm{Ker}(v)$ et $\mathrm{Im}(v)$ sont stables par u.

Corollaire 11 : u et $P(u)$ commutent avec $P \in \mathbb{K}[X]$ et donc $\mathrm{Ker}(P(u))$ est stable par u.

Corollaire 12 : Les sous-espaces propres sont stables par u.

Exemple 13 : Les sous-espaces caractéristiques sont stables par u.

Proposition 14 : F est stable par u si et seulement si F° est stable par ${}^t u$.

Proposition 15 : Lemme des noyaux.

II/ Diagonalisation et trigonalisation.

A/ Réduction d'un endomorphisme. [ROM]

Définition 16 : Trigonalisable.

Proposition 17 : u est trigonalisable si et seulement si χ_u est scindé.

Corollaire 18 : Si u est trigonalisable, F stable par u alors $u|_F$ est trigonalisable.

Définition 19 : Endomorphismes diagonalisables.

Proposition 20 : Caractérisations des endomorphismes diagonalisables.

Corollaire 21 : Si F est stable par u alors $u|_F$ est diagonalisable.

B/ Réduction d'une famille d'endomorphismes. [ROM]

Théorème 22 : Diagonalisation et trigonalisation simultané : Si u et v commutent et sont diagonalisables (resp. trigonalisables) alors u et v sont codiagonalisables (resp. cotrigonalisables).

Remarque 23 : La réciproque dans le cas diagonalisable est vraie mais pas dans le cas trigonalisable.

Application 24 : Si u et v commutent et sont diagonalisables alors $u+v$ est diagonalisable.

III/ Réductions en sous-espaces stables.

A/ Décomposition de Dunford. [ROM]

Théorème 25 : Décomposition de Dunford.

B/ Réduction de Jordan. [ROM]

Développement 1

Lemme 26 : $E_{f,x} = \mathrm{Vect}(x, f(x), \ldots, f^{p-1}(x))$ est stable par f.

Théorème 27 : Réduction de Jordan dans le cas nilpotent.

Corollaire 28 : Dans le cas général.

C/ Réduction de Frobenius. [G] [ROM]

Définition 29 : Endomorphismes cycliques.

Définition 30 : Matrice compagnon.

Proposition 31 : Si f est cyclique alors il existe une base $\mathcal{B}$ telle que $\mathrm{Mat}_{\mathcal{B}}(f)$ soit une matrice compagnon.

Théorème 32 : Réduction de Frobenius.

Corollaire 33 : f et g sont semblables si et seulement si f et g ont les mêmes invariants de similitude.

D/ Réduction des endomorphismes normaux. [ROM]

Définition 34 : Endomorphismes normaux, symétriques, antisymétriques.

Développement 2

Théorème 35 : Réduction des endomorphismes normaux.

Corollaire 36 : Cas symétrique, antisymétrique et orthogonal.

Références :

— [G] Gourdon Algèbre p. 162 et p. 289

— [OBJ] Objectif Agrégation p. 157

— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 675-702, p. 743

Leçon n°152 : Endomorphismes diagonalisables en dimension finie.

Soit $\mathbb{K}$ un corps et E un $\mathbb{K}$-ev de dimension finie $n \geq 1$ et pour $u \in \mathcal{L}(E)$, on pose χ_u et μ_u son polynôme caractéristique et minimal.

I/ Généralités sur les endomorphismes diagonalisables.

A/ Espaces et éléments propres. [BER]

Définition 1 : Valeur propre, vecteur propre et spectre.

Proposition 2 : Valeur propre $\Leftrightarrow$ racine de χ_u et donc $\mathrm{Sp}_{\mathbb{K}}(u)$ est fini.

Proposition 3 : Relation multiplicité valeur propre et dimension de l'espace propre.

Lemme 4 : Les sous-espaces propres de u sont en somme directe.

B/ Diagonalisabilité. [BER]

Définition 5 : Endomorphisme diagonalisable.

Remarque 6 : Définition matricielle de la diagonalisabilité, si M est diagonalisable alors M contient une matrice diagonale dans sa classe de similitude.

II/ Critères de diagonalisation.

A/ Critère sur les sous-espaces propres. [BER] [G]

Théorème 7 : Lemme des noyaux.

Théorème 8 : Propriétés équivalentes de diagonalisation.

Corollaire 9 : Si u possède n valeurs propres distinctes, alors u est diagonalisable.

Exemple 10 : $u : (x_1, \ldots, x_n) \mapsto (x_1, 2x_2 + x_1, \ldots, nx_n + \sum_{k=1}^{n-1} x_k)$ est diagonalisable car il a n valeurs propres distinctes.

Exemple 11 : Diagonalisation des endomorphismes circulants.

Méthode 12 : Méthode générale pour diagonaliser une matrice lorsque l'on sait calculer ses valeurs propres.

Exemple 13 : Diagonalisation de $J_n = (1)$: $\chi_{J_n} = X^{n-1}(X-n)$, or $\dim(E_0(J_n)) = n-1$ et $\dim(E_n(J_n)) = 1$ donc J_n est diagonalisable.

B/ Critère sur les polynômes d'endomorphismes. [BER] [CAL] [ROM]

Lemme 14 : Si λ est une valeur propre et P annule u, alors λ est racine de P.

Corollaire 15 : Les polynômes μ_u et χ_u ont les mêmes racines qui sont les valeurs propres de u.

Théorème 16 : Propriétés équivalentes de diagonalisation.

Corollaire 17 : Si F est stable par u et que u est diagonalisable, alors $u|_F$ est diagonalisable.

Développement 1

Application 18 : Dénombrement des endomorphismes diagonalisables de $\mathbb{F}_q^n$.

Application 19 : Calcul de l'exponentielle d'une matrice diagonalisable avec le polynôme interpolateur de Lagrange.

III/ Propriétés issues de la diagonalisation.

A/ Propriétés topologiques. [ROM] [OBJ]

On prend ici $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Notation 20 : Notation de l'ensemble des endomorphismes diagonalisables sur $\mathbb{K}$ et ceux à valeurs propres deux à deux différentes.

Théorème 21 : $D_n'(\mathbb{C})$ et $D_n(\mathbb{C})$ sont denses dans $\mathrm{M}_n(\mathbb{C})$ et l'intérieur de $D_n(\mathbb{C})$ est $D_n'(\mathbb{C})$.

Corollaire 22 : Théorème de Cayley-Hamilton, vrai pour $\mathbb{K}$ quelconque.

Définition 23 : Endomorphismes trigonalisables et notations $T_n(\mathbb{R})$.

Proposition 24 : $T_n(\mathbb{R})$ est fermé et l'adhérence de $D_n(\mathbb{R})$ est $T_n(\mathbb{R})$.

Proposition 25 : L'application $A \mapsto \mu_A$ n'est pas continue pour $n \geq 2$.

B/ Décomposition de Dunford. [BER]

Définition 26 : Sous-espaces caractéristiques.

Proposition 27 : Ils sont en somme directe et engendrent tout l'espace.

Lemme 28 : Les projecteurs spectraux sont des polynômes en u.

Théorème 29 : Décomposition de Dunford.

Développement 2

Proposition 30 : Décomposition de Dunford par la méthode de Newton.

C/ Codiagonalisation. [ROM] [OBJ]

Théorème 31 : Codiagonalisation simultanée.

Remarque 32 : Écriture matricielle.

Corollaire 33 : Sous-groupe fini de $\mathrm{GL}_m(\mathbb{K})$.

Corollaire 34 : Si u et v sont diagonalisables et commutent, alors $u+v$ est diagonalisable.

D/ Application aux portraits de phases. [BERT]

On se place ici dans le cas où $A \in \mathrm{M}_2(\mathbb{R})$.

Application 35 : La classification des portraits de phase du système différentiel $\begin{pmatrix} x \\ y \end{pmatrix}' = A \begin{pmatrix} x \\ y \end{pmatrix}$ est mise en annexe.

IV/ Diagonalisation des endomorphismes autoadjoints [ROM] [PGCD]

On suppose connu les notions d'adjoints. Si $u \in \mathcal{L}(E)$, on note u^* son adjoint et on se place ici pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Théorème 36 : Théorème spectral

Exemple 37 : Exemple de matrice symétrique qui est donc diagonalisable.

Application 38 : Matrice Hessienne et recherche d'extrema.

Références :

— [G] Gourdon Algèbre p. 161
— [OBJ] Objectif Agrégation p. 178 et p. 206
— [BER] Berhuy Algèbre le grand combat p. 941
— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 682
— [BERT] Berthelin Équations différentielles p. 203
— [CAL] Caldéro Histoires hédonistes tome 1 p. 264
— [PGCD] Rouvière Petit Guide du Calcul Différentiel p. 283

Leçon n° 153 : Valeurs propres, vecteurs propres. Calculs exacts ou approchés d'éléments propres. Applications.

Soit $\mathbb{K}$ un corps, $A \in \mathrm{M}_n(\mathbb{K})$ et $n \geq 1$.

I/ Éléments propres d'une matrice.

A/ Définitions et calculs exacts. [G] [FGNAlg2]

Définition 1 : Valeur propre, vecteur propre et spectre.

Définition 2 : Sous-espaces propres.

Théorème 3 : Somme directe des sous-espaces propres.

Définition 4 : Polynôme caractéristique.

Proposition 5 : Valeur propre si et seulement si racine du polynôme caractéristique.

Exemple 6 : Cas $n = 2$ et expression du polynôme caractéristique et donc les valeurs propres.

Proposition 7 : Algorithme de Fadeev-Le-Verrier : algorithme en $O(n^4)$ opérations permettant d'obtenir les coefficients du polynôme caractéristique.

Remarque 8 : Calculer les valeurs propres demande de trouver les racines d'un polynôme, ce qui est difficile en pratique.

B/ Cas particuliers de calcul d'éléments propres. [G]

Développement 1

Proposition 9 : Déterminant circulant.

Application 10 : Suite de polygones.

Proposition 11 : Matrices compagnons.

Proposition 12 : Matrices nilpotentes.

Proposition 13 : Les valeurs propres des matrices symétriques réelles sont réelles.

Proposition 14 : Cas des matrices stochastiques.

C/ Application à la réduction. [G] [ROM]

Théorème 15 : Théorème spectral.

Proposition 16 : A est diagonalisable si et seulement si les sous-espaces propres sont en somme directe et engendrent l'espace.

Application 17 : Calcul d'une puissance de matrice.

Application 18 : Étudier la convergence des suites $U_{n+1} = AU_n$ car $U_n = A^n U_0$ et si $(A^n)_{n\in\mathbb{N}}$ converge alors $(U_n)_{n\in\mathbb{N}}$ converge aussi.

Application 19 : Calcul de l'exponentielle de matrice.

II/ Recherche approchée d'éléments propres.

A/ Normes matricielles et conditionnement. [ALL]

Définition 20 : Norme matricielle.

Définition 21 : Rayon spectral.

Proposition 22 : $\rho(A) \leq \|A\|$ et réciproque partielle.

Proposition 23 : $A^n \to 0 \Leftrightarrow \rho(A) < 1$.

Définition 24 : Conditionnement.

Remarque 25 : Permet d'avoir une mesure de l'erreur lors de méthode itérative.

Proposition 26 : Inégalité avec conditionnement.

B/ Localisation de valeurs propres. [FGNAlg2]

Développement 2

Théorème 27 : Disques de Gershgörin.

Application 28 : Son application avec le déterminant d'une matrice.

Proposition 29 : Si un disque est isolé, alors il y a une unique valeur propre dans ce disque.

Remarque 30 : En utilisant les disques de Gershgörin sur une matrice compagnon on peut donc localiser les racines d'un polynôme.

C/ Méthodes itératives. [ALL] [CIA]

Proposition 31 : Méthode de la puissance.

Proposition 32 : Méthode de la puissance inverse.

Proposition 33 : Méthode QR.

Références :

— [G] Gourdon Algèbre p. 146, p. 161, p. 221

— [FGNAlg2] Francinou, Gianella Nicolas Algèbre 2 p. 79-80

— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 682

— [ALL] Allaire Analyse numérique p. 410-415, p. 440

— [CIA] Ciarlet Introduction à l'analyse numérique matricielle p. 123

Leçon n° 154 : Exemples de décompositions de matrices. Applications.

$\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I/ Résolution de systèmes linéaires.

A/ Par élimination de Gauss. [CIA] [CAL] [FGNAlg2]

Proposition 1 : Si T est triangulaire, l'algorithme de remontée s'effectue en $O(n^2)$ opérations sur le corps $\mathbb{K}$.

Définition 2 : Matrices de transvections et dilatations (matrices élémentaires).

Remarque 3 : Opération sur les lignes $\leftrightarrow$ multiplication à gauche, opération sur les colonnes $\leftrightarrow$ multiplication à droite.

Théorème 4 : $\mathrm{SL}_n(\mathbb{K})$ est engendré par les transvections. $\mathrm{GL}_n(\mathbb{K})$ est engendré par les transvections et dilatations.

Théorème 5 : Si A est une matrice rectangulaire, $A = PE$ où P est inversible et E est échelonnée réduite.

Remarque 6 : En utilisant cette décomposition (calculable en $O(n^3)$ opérations), on peut résoudre un système en $O(n^3)$ opérations en le couplant avec l'algorithme de remontée.

Application 7 : Calcul de l'inverse et du déterminant en $O(n^3)$ opérations.

B/ Décomposition LU. [CIA]

Proposition 8 : Décomposition LU si les mineurs principaux sont non nuls.

Remarque 9 : La décomposition LU se calcule en $O(n^3)$ opérations.

Application 10 : Résolution de plusieurs systèmes linéaires avec la même matrice A : on résout $Lw = b$ puis $Uu = w$ et donc pour résoudre n systèmes avec la même matrice A l'algorithme nécessite $O(n^3)$ opérations (contrairement à $O(n^4)$ avec l'algorithme de Gauss).

Application 11 : Calcul du déterminant en $O(n^3)$ opérations.

Exemple 12 : Si $A \in S_n^{++}(\mathbb{R})$ alors A admet une décomposition LU.

Remarque 13 : Toute matrice inversible admet une décomposition PLU où P est une matrice de permutation : il suffit de permuter les lignes de telle sorte à se ramener à une matrice ayant les mineurs principaux non nuls.

C/ Décomposition de Cholesky (cas de $S_n^{++}(\mathbb{R})$) [CIA]

Proposition 14 : Décomposition de Cholesky.

Remarque 15 : La preuve utilise la décomposition LU.

Remarque 16 : L'algorithme pour trouver la décomposition est plus efficace que LU (toujours en $O(n^3)$ mais coûte deux fois moins d'opérations que LU).

D/ Décomposition QR. [FGNAlg3]

Proposition 17 : Factorisation QR.

Remarque 18 : Issue du processus d'orthonormalisation de Gram-Schmidt qui en donne une méthode de calcul.

II/ Réductions d'endomorphismes.

A/ Décomposition de Dunford. [BER] [ROM]

Lemme 19 : Lemme des noyaux.

Définition 20 : Sous-espaces caractéristiques.

Théorème 21 : Décomposition de Dunford.

Développement 1

Proposition 22 : Décomposition de Dunford effective.

B/ Réduction de Jordan. [ROM]

Définition 23 : Blocs de Jordan.

Théorème 24 : Réduction de Jordan pour les nilpotents.

Corollaire 25 : Réduction de Jordan dans le cas général.

C/ Applications. [ROM]

Application 26 : Calcul de l'exponentielle de matrice.

Application 27 : Résolution du système différentiel $Y' = AY$.

Application 28 : Calcul de la puissance d'une matrice grâce au binôme de Newton et Dunford.

III/ Décomposition polaire. [CAL]

Développement 2

Théorème 29 : La décomposition polaire est un homéomorphisme.

Théorème 30 : Dans le cas complexe aussi.

Remarque 31 : Écriture dans le cas $n = 1$ qui vient de l'écriture sous forme polaire des complexes.

Application 32 : $|||A|||_2 = \sqrt{\rho(A^T A)}$.

Application 33 : Tout sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$ contenant $O_n(\mathbb{R})$ est $O_n(\mathbb{R})$.

Application 34 : $\mathrm{Conv}(\mathrm{O}_n(\mathbb{R})) = \mathrm{B}_{|||\cdot|||_2}(0, 1)$

Références :

- [CAL] Caldéro Nouvelles Histoires Hédonistes tome 1 p. 203, p. 213, p. 347
- [FGNAlg2] Francinou Gianella Nicolas Algèbre 2 p. 177
- [FGNAlg3] Francinou Gianella Nicolas Algèbre 3 p. 40
- [CIA] Ciarlet Introduction à l'analyse numérique matricielle p. 72-90, p. 92
- [BER] Berhuy Algèbre le grand combat p. 941
- [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 611 et p. 681

Leçon n° 155 : Exponentielle de matrices. Applications.

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I/ Convergence et propriétés algébriques.

A/ Définition et propriétés générales. [ROM] [CAL]

Proposition 1 : L'exponentielle matricielle est bien définie.

Exemple 2 : Calcul pour A nilpotente.

Exemple 3 : Calcul pour une matrice diagonale.

Proposition 4 : $e^A \in \mathbb{K}[A]$.

Proposition 5 : Si $P \in \mathrm{GL}_n(\mathbb{K})$, si $A = PBP^{-1}$ alors $e^A = Pe^BP^{-1}$.

Corollaire 6 : $\det(e^A) = e^{\mathrm{Tr}(A)}$ et e^A est inversible avec pour inverse e^{-A}.

Application 7 : Calcul de l'exponentielle matricielle si la matrice est diagonalisable.

Proposition 8 : Si A et B commutent alors $e^{A+B} = e^Ae^B$.

Proposition 9 : $\overline{e^A} = e^{\overline{A}}$.

Proposition 10 : ${}^te^A = e^{{}^tA}$.

Corollaire 11 : Si $A \in S_n(\mathbb{R})$ alors $e^A \in S_n(\mathbb{R})$, si $A \in A_n(\mathbb{R})$ alors $e^A \in \mathrm{SO}_n(\mathbb{R})$.

Proposition 12 : $\exp(A_n(\mathbb{R})) = \mathrm{SO}_n(\mathbb{R})$.

B/ De Dunford au calcul d'exp. [ROM] [GRIF] [FGNAlg2]

Théorème 13 : Décomposition de Dunford.

Théorème 14 : Dunford multiplicatif.

Remarque 15 : Lien entre les deux.

Proposition 16 : Décomposition exponentielle de Dunford.

Corollaire 17 : A est diagonalisable si et seulement si e^A est diagonalisable.

Application 18 : $\exp^{-1}(I_n) = \{M \in \mathrm{D}_n(\mathbb{C}),\ \mathrm{Sp}(M) \subset 2i\pi\mathbb{Z}\}$.

Application 19 : Calcul de l'exponentielle de matrice en utilisant la décomposition de Dunford.

II/ Propriétés analytiques de l'exponentielle matricielle.

A/ Différentiabilité. [ROM]

Théorème 20 : exp est C^1 et calcul de sa différentielle.

Proposition 21 : exp est un C^1 difféomorphisme local entre un voisinage de 0 et un voisinage de I_n.

Application 22 : Logarithme matriciel.

B/ Injectivité et surjectivité. [ROM] [ZAV] [CAL]

Proposition 23 : $\exp : \mathrm{M}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$ n'est ni surjective (car à valeurs dans $\mathrm{GL}_n^+(\mathbb{R})$) ni injective.

Contre-exemple 24 : $R(\theta) = \exp\left(\begin{pmatrix} 0 & \theta \\ \theta & 0 \end{pmatrix}\right)$.

Développement 1

Lemme 25 : $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$.

Proposition 26 : $\exp : \mathrm{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est surjective.

Contre-exemple 27 : L'exponentielle matricielle complexe n'est pas injective.

Application 28 : $\exp(\mathrm{M}_n(\mathbb{R})) = \{M^2,\ M \in \mathrm{GL}_n(\mathbb{R})\}$.

Application 29 : $\mathrm{GL}_n(\mathbb{C})$ est connexe par arcs.

Application 30 : Si $p \neq 0$ alors $\forall A \in \mathrm{M}_n(\mathbb{C})$, $\exists X \in \mathbb{C}[A]$ tel que $A = X^p$.

Proposition 31 : $\exp : D_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$ est injective.

C/ Dans $S_n^{++}(\mathbb{R})$ et $H_n^{++}(\mathbb{C})$. [CAL]

Développement 2

Proposition 32 : $\exp : S_n(\mathbb{R}) \to S_n^{++}(\mathbb{R})$ est un homéomorphisme.

Proposition 33 : $\exp : H_n(\mathbb{C}) \to H_n^{++}(\mathbb{C})$ est un homéomorphisme.

Corollaire 34 : $S \mapsto \sqrt{S}$ est un homéomorphisme.

Proposition 35 : Décomposition polaire.

Remarque 36 : Dans le cas $n = 1$ on retrouve la décomposition polaire d'un complexe.

Corollaire 37 : $\mathrm{GL}_n(\mathbb{R}) \overset{\text{homéo}}{\simeq} O_n(\mathbb{R}) \times \mathbb{R}^{\frac{n(n+1)}{2}}$ et $\mathrm{GL}_n(\mathbb{C}) \overset{\text{homéo}}{\simeq} U_n(\mathbb{C}) \times \mathbb{R}^{n^2}$.

III/ Application aux EDL. [G] [GRIF] [PGCD]

Proposition 38 : $t \mapsto e^{tA}$ est de classe C^∞ et de dérivée $t \mapsto Ae^{tA} = t \mapsto e^{tA}A$.

Proposition 39 : Si $A \in \mathrm{M}_n(\mathbb{K})$, $Y' = AY$ a ses solutions maximales définies sur $\mathbb{R}$ et expression solution.

Remarque 40 : On peut toujours se ramener à l'ordre 1.

Théorème 41 : Théorème de stabilité de Liapounov

Références :

— [CAL] Caldéro Histoires Hédonistes tome 1 p. 207-210
— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 759-772
— [GRIF] Grifone Algèbre linéaire p. 373-377
— [FGNAlg2] Francinou Gianella Nicolas Algèbre 2 p.247
— [ZAV] Zavidovique Un max de maths p. 48
— [G] Gourdon Analyse p. 360
— [PGCD] Rouvière Petit Guide du Calcul Différentiel p. 130

Leçon n° 156 : Endomorphismes trigonalisables. Endomorphismes nilpotents.

$\mathbb{K}$ un corps et E un $\mathbb{K}$-ev de dimension finie $n \geq 1$, $u \in \mathcal{L}(E)$.

I/ Rappels sur les polynômes d'endomorphismes. [MAN]

Théorème 1 : L'application $\mathbb{K}[X] \to \mathcal{L}(E)$ est un morphisme de $\mathbb{K}$-algèbres et son image est $\mathbb{K}[u]$.

Proposition 2 : L'idéal annulateur est engendré par le polynôme minimal.

Remarque 3 : C'est vrai pour les matrices.

Définition 4 : Polynôme caractéristique.

Proposition 5 : λ est une valeur propre de u si et seulement si $\chi_u(\lambda) = 0$.

Proposition 6 : Si F est stable alors $\chi_{u|_F}$ divise χ_u et il en est de même pour le polynôme minimal.

Théorème 7 : Théorème de Cayley-Hamilton.

Lemme 8 : Lemme des noyaux.

II/ Endomorphismes trigonalisables.

A/ Caractérisations. [ROM]

Définition 9 : Endomorphismes trigonalisables.

Proposition 10 : u est trigonalisable si et seulement si χ_u est scindé.

Exemple 11 : Dans $\mathbb{C}$, qui est algébriquement clos, tous les endomorphismes sont trigonalisables.

Exemple 12 : La matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est trigonalisable sur $\mathbb{C}$ mais pas sur $\mathbb{R}$.

Corollaire 13 : Si F est u-stable et u est trigonalisable alors $u|_F$ est trigonalisable.

Corollaire 14 : La trace est la somme des valeurs propres et le déterminant le produit.

B/ Cotrigonalisation. [ROM]

Lemme 15 : Si $uv = vu$ alors $\mathrm{Ker}(v)$ et $\mathrm{Im}(v)$ sont u-stables.

Proposition 16 : Cotrigonalisation.

Exemple 17 : Si u et v commutent et sont trigonalisables alors $u+v$ est trigonalisable.

C/ Propriétés topologiques. [ROM]

Proposition 18 : $\overline{D_n(\mathbb{R})} = T_n(\mathbb{R})$.

Proposition 19 : $D_n(\mathbb{C})$ est dense dans $M_n(\mathbb{C})$.

III/ Endomorphismes nilpotents.

A/ Caractérisations. [ROM]

Définition 20 : Endomorphismes nilpotents.

Exemple 21 : Exemple où $\mu_u = X^p$ et $\chi_u = X^n$.

Proposition 22 : u est nilpotent diagonal si et seulement si $u = 0$.

Proposition 23 : $p \leq n$ et l'égalité a lieu si et seulement si $\dim(\mathrm{Ker}(u)) = 1$.

Application 24 : Si u est nilpotent d'ordre n, u est trigonalisable et sa matrice dans la base $(x, f(x), \ldots, f^{n-1}(x))$ où $f^{n-1}(x) \neq 0$ est un bloc de Jordan.

Proposition 25 : u est nilpotent si et seulement si pour tout $k \in [\![1,n]\!]$, $\mathrm{Tr}(u^k) = 0$.

Corollaire 26 : Si F est u-stable et u est nilpotent alors $u|_F$ est nilpotent.

Proposition 27 : Si $uv = vu$ et sont nilpotents alors $u+v$ et uv sont nilpotents.

B/ Réduction des endomorphismes nilpotents. [ROM]

Développement 1

Théorème 28 : Théorème de réduction de Jordan pour les nilpotents.

Corollaire 29 : Théorème de réduction de Jordan dans le cas général.

Corollaire 30 : Deux endomorphismes trigonalisables sont semblables si et seulement s'ils ont la même réduction de Jordan.

C/ Noyaux itérés et tableaux de Young. [MAN]

Proposition 31 : Suite des noyaux itérés.

Proposition 32 : La suite des différences est décroissante.

Définition 33 : Tableau de Young et cas des endomorphismes nilpotents (annexe).

Proposition 34 : Si $d_1 \geq \cdots \geq d_r$, $\mathrm{diag}(J_{d_1}, \ldots, J_{d_r})$ est nilpotent d'ordre d_1.

Proposition 35 : Lien entre tableau de Young et réduction de Jordan.

Théorème 36 : Deux endomorphismes nilpotents sont semblables si et seulement s'ils ont les mêmes tableaux de Young.

IV/ Décomposition de Dunford. [ROM] [BER]

Proposition 37 : Décomposition de Dunford.

Développement 2

Proposition 38 : Algorithme de décomposition de Dunford via méthode de Newton.

Application 39 : Calcul de l'exponentielle de matrice.

Application 40 : Résolution de $Y' = AY$.

Références :

- [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 675-682, p. 685
- [MAN] Mansuy p. 1-48, p. 93, p. 107-117
- [BER] Berhuy Algèbre le grand combat p. 941

Leçon n° 157 : Matrices symétriques réelles, matrices hermitiennes.

I/ Matrices symétriques et hermitiennes

A/ Définition et propriétés générales. [G] [ROM]

Définition 1 : Matrice symétrique et matrice hermitienne.

Exemple 2 : Exemple de telles matrices.

Proposition 3 : L'ensemble $\mathrm{S}_n(\mathbb{R})$ est un espace vectoriel sur $\mathbb{R}$ de dimension $\frac{n(n+1)}{2}$ et $H_n(\mathbb{C})$ est un espace vectoriel sur $\mathbb{R}$ de dimension n^2.

Proposition 4 : On a $\mathrm{M}_n(\mathbb{R}) = S_n(\mathbb{R}) \oplus A_n(\mathbb{R})$ et $\mathrm{M}_n(\mathbb{C}) = S_n(\mathbb{R}) \oplus iA_n(\mathbb{R})$.

Définition 5 : Matrices symétriques (hermitiennes) positives et matrices définies positives.

Proposition 6 : Leurs spectres sont réels.

B/ Lien avec les formes quadratiques et hermitiennes. [G]

Définition 7 : Forme bilinéaire symétrique et forme quadratique.

Définition 8 : Forme sésquilinéaire à géométrie hermitienne et forme hermitienne.

Proposition 9 : Unicité de la forme polaire et formules de polarisation.

Remarque 10 : Lien avec les matrices.

Exemple 11 : Écrire la matrice de deux formes quadratiques / hermitiennes.

Définition 12 : Forme quadratique q définie (positive).

Proposition 13 : Lien entre une matrice définie positive et une forme quadratique définie positive.

II/ Réduction et applications

A/ Orthogonalité et théorème spectral. [G] [ROM] [FGNAlg3]

Définition 14 : Base q-orthogonale.

Théorème 15 : Existence d'une telle base.

Corollaire 16 : Il existe $P \in \mathrm{GL}_n(\mathbb{K})$ tel que ${}^tPAP$ soit diagonale.

Théorème 17 : Théorème spectral.

Application 18 : Existence de la racine carrée.

Application 19 : Lien entre les valeurs propres et le caractère positif.

Développement 1

Proposition 20 : Diagonalisation simultanée.

Lemme 21 : log-concavité du déterminant sur $S_n^{++}(\mathbb{R})$.

Application 22 : Ellipsoïde de John-Loewner.

B/ Signature d'une forme quadratique et hermitienne. [G] [ROM]

Théorème 23 : Réduction de Gauss.

Exemple 24 : Exemple de réduction.

Théorème 25 : Sylvester et signature.

Exemple 26 : Avec l'exemple précédent, signature.

Corollaire 27 : Congruence et nombre de classes d'équivalence pour l'action.

III/ Propriétés topologiques des matrices symétriques réelles. [ROM]

Proposition 28 : Critère de Sylvester.

Remarque 29 : Critère simple pour vérifier qu'une matrice symétrique est définie positive informatiquement.

Corollaire 30 : $S_n^{++}(\mathbb{R})$ est un ouvert de $\mathrm{M}_n(\mathbb{R})$.

Théorème 31 : Décomposition polaire.

Application 32 : $\mathrm{GL}_n(\mathbb{R}) \overset{\text{homéo}}{\simeq} O_n(\mathbb{R}) \times \mathbb{R}^{\frac{n(n+1)}{2}}$.

Application 33 : $O_n(\mathbb{R})$ est le seul sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$ contenant $O_n(\mathbb{R})$.

Application 34 : Calcul de $|||A|||_2 = \sqrt{\rho({}^tAA)}$.

Définition 35 : Exponentielle de matrice.

Exemple 36 : Exponentielle d'une matrice diagonale.

Développement 2

Théorème 37 : $\exp : S_n(\mathbb{R}) \to S_n^{++}(\mathbb{R})$ est un homéomorphisme.

IV/ Applications à d'autres domaines

A/ Différentielle seconde. [PGCD]

Théorème 38 : Schwarz.

Définition 39 : Hessienne qui est donc symétrique.

Théorème 40 : Conditions nécessaires et suffisantes pour un extremum.

Application 41 : Cas particulier pour $n = 2$.

B/ En analyse numérique. [CIA]

Proposition 42 : Décomposition LU.

Remarque 43 : Complexité pour n systèmes linéaires similaires : $O(n^3)$ opérations.

Proposition 44 : Décomposition de Cholesky.

Remarque 45 : Toujours une complexité de $O(n^3)$ opérations mais deux fois moins d'opérations pour les matrices symétriques.

Références :

— [G] Gourdon Algèbre p. 227-240
— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 732-743
— [PGCD] Rouvière Petit Guide du Calcul Différentiel p. 283 et p. 360
— [CIA] Ciarlet Introduction à l'analyse numérique matricielle p. 82-90
— [FGNAlg3] Fracinou, Gianella Nicolas Algèbre 3 p. 229

Leçon n° 158 : Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie).

Soit $(E, \langle\cdot,\cdot\rangle)$ un espace euclidien de dimension $n \geq 1$ et on note $||\cdot||$ sa norme associée et soit $u \in \mathcal{L}(E)$.

I/ Endomorphismes d'un espace euclidien.

A/ Adjoint d'un endomorphisme. [ROM]

Théorème 1 : Existence et unicité de l'adjoint.

Proposition 2 : Matrice du produit scalaire.

Proposition 3 : Propriétés de l'adjoint.

B/ Exemples d'endomorphismes remarquables. [ROM]

Définition 4 : Isométries.

Proposition 5 : u isométrie si et seulement si u est linéaire et conserve la norme.

Exemple 6 : Les homothéties qui sont des isométries sont $\pm Id$, les symétries orthogonales et rotations sont des isométries, les valeurs propres des isométries ne peuvent qu'être ± 1

Proposition 7 : Matrice orthogonale et lien avec adjoint pour isométrie.

Définition 8 : Endomorphismes symétriques et antisymétriques.

Proposition 9 : Si $u \in \mathcal{L}(E)$ alors $\frac{u+u^*}{2} \in \mathrm{S}(E)$ et $\frac{u-u^*}{2} \in \mathcal{A}(E)$.

Définition 10 : Endomorphismes normaux.

Exemple 11 : Les isométries, auto-adjoints sont normaux.

Proposition 12 : Caractérisation matricielle des différents endomorphismes dans une BON.

II/ Cas des endomorphismes normaux. [ROM]

Lemme 13 : Si F stable par u normal alors $F^\perp$ stable par u.

Lemme 14 : $\forall u \in \mathcal{L}(E)$ normal, $\exists P$ de dim 1 ou 2 u-stable.

Développement 1

Théorème 15 : Réduction des endomorphismes normaux.

Application 16 : Réduction des endomorphismes antisymétriques.

III/ Étude des endomorphismes autoadjoints/symétriques.

A/ Premières propriétés. [ROM]

Proposition 17 : Dimension de $S(E)$ et $\mathcal{A}(E)$.

Définition 18 : Endomorphismes autoadjoints positifs et définis positifs.

Exemple 19 : La matrice du produit scalaire est définie positive.

Proposition 20 : Si $S \in S_n(\mathbb{R})$, $\mathrm{Sp}_{\mathbb{C}}(S) \subset \mathbb{R}$.

Lemme 21 : Les sous-espaces propres sont orthogonaux.

B/ Autour du théorème spectral. [ROM] [CAL]

Théorème 22 : Théorème spectral.

Corollaire 23 : Si $u \in S(E)$ caractérisation de la positivité de u selon la positivité des valeurs propres.

Application 24 : Si $A \in S_n(\mathbb{R})$, $|||A|||_2 = \rho(A)$.

Application 25 : Existence racine carrée pour les positives.

Proposition 26 : Critère de Sylvester : $A \in \mathrm{S}_n^{++}(\mathbb{R})$ si et seulement si les mineurs principaux de A sont tous strictement positifs.

Corollaire 27 : $S_n^{++}(\mathbb{R})$ est un ouvert de $\mathrm{M}_n(\mathbb{R})$.

Développement 2

Théorème 28 : $\exp : S_n(\mathbb{R}) \to S_n^{++}(\mathbb{R})$ est un homéomorphisme.

Application 29 : $S \mapsto \sqrt{S}$ est un homéomorphisme dans $S_n^{++}(\mathbb{R})$.

IV/ Endomorphismes orthogonaux.

A/ Réduction et structure de groupe. [ROM]

Proposition 30 : u isométrie si et seulement si elle envoie toute BON sur une BON.

Théorème 31 : Réduction des isométries.

Proposition 32 : $O(E)$ sous-groupe de $\mathcal{L}(E)$.

Définition 33 : Symétries orthogonales, réflexions, renversements.

Théorème 34 : $O(E)$ est engendré par les réflexions et $SO(E)$ par les renversements.

B/ Propriétés topologiques. [ROM] [CAL]

Proposition 35 : $O(E)$ compact de $\mathcal{L}(E)$.

Proposition 36 : Les composantes connexes de $O(E)$ sont $SO(E)$ et $O^-(E)$.

Théorème 37 : Décomposition polaire.

Application 38 : $|||A|||_2 = \sqrt{\rho({}^tAA)}$.

Application 39 : Le seul sous-groupe compact de $\mathrm{GL}_n(\mathbb{R})$ contenant $O_n(\mathbb{R})$ est $O_n(\mathbb{R})$.

Références :

— [CAL] Caldéro Histoires Hédonistes tome 1 p. 201 et p. 208

— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 713-747

Leçon n° 159 : Formes linéaires et dualité en dimension finie. Exemples et applications.

I/ Formes linéaires et espace dual.

A/ Généralités sur les formes linéaires. [ROM] [G]

Définition 1 : Forme linéaire et E^*.

Exemple 2 : Les projections sont des formes linéaires.

Exemple 3 : $A \mapsto \mathrm{Tr}(AM)$ où $M \in \mathrm{M}_n(\mathbb{R})$ est une forme linéaire sur $\mathrm{M}_n(\mathbb{R})$.

Proposition 4 : Le noyau d'une forme linéaire est un hyperplan et réciproque.

Proposition 5 : Si l_1 et l_2 deux formes linéaires telles que $\mathrm{Ker}(l_1) \subset \mathrm{Ker}(l_2)$ alors l_1 et l_2 sont proportionnelles.

B/ Espace dual et base duale. [ROM] [G]

Proposition 6 : $\dim(E^*) = \dim(E)$ et base duale.

Exemple 7 : Base duale de la base canonique de $\mathbb{K}^n$ et base duale de la base canonique de $\mathbb{K}_n[X]$.

Théorème 8 : Théorème de représentation de Riesz en dimension finie.

Application 9 : Isomorphisme canonique entre E et E^* si E euclidien via $x \mapsto \langle x, \cdot \rangle$.

Développement 1.a)

Proposition 10 : $\mathrm{M}_n(\mathbb{R})^*$.

C/ Bidual et bases antéduales. [ROM] [G]

Proposition 11 : Isomorphisme entre E et E^{**}.

Remarque 12 : C'est un isomorphisme canonique car ne dépend pas de la base choisie.

Proposition 13 : Existence et unicité de la base antéduale.

Remarque 14 : Nous verrons un moyen par la suite de la calculer en pratique.

II/ Orthogonalité.

A/ Notions d'orthogonalités. [G]

Définition 15 : $X^\perp$ et Y°.

Remarque 16 : Si $\varphi \in E^*$ alors $\{\varphi\}^\circ = \mathrm{Ker}(\varphi)$.

Proposition 17 : Si $A \subset B$ alors $B^\perp \subset A^\perp$ et toutes les autres propriétés.

Proposition 18 : $\dim(F^\perp) + \dim(F) = \dim(E)$ et pareil pour le rond.

Proposition 19 : Prop $\perp$ et $\circ$ pour $\cap$ et $+$.

Théorème 20 : Lien entre intersections d'hyperplans et sev de dimension donnée.

Application 21 : Système d'équations pour un sev, par la méthode du pivot de Gauss on peut à partir d'un sev trouver ces équations et donc les formes linéaires associées.

B/ Transposée d'une application linéaire. [G]

Définition 22 : Application transposée.

Proposition 23 : Propriétés sur l'application transposée.

Proposition 24 : Composition.

Proposition 25 : F stable par $u \iff F^\perp$ stable par ${}^t u$.

Remarque 26 : Utile pour des démonstrations par récurrence se faisant sur la dimension.

Proposition 27 : Vision matricielle.

Proposition 28 : Si M matrice dont les colonnes sont les vecteurs de la base duale $\mathcal{B}^*$ alors ${}^t M^{-1}$ a pour colonnes les vecteurs de la base antéduale $\mathcal{B}$.

III/ Applications de la dualité.

A/ Application à la réduction. [ROM]

Développement 2

Théorème 29 : Réduction de Jordan pour les nilpotents.

Corollaire 30 : Réduction de Jordan dans le cas général.

B/ Convexité. [OBJ] [ZQ]

Lemme 31 : Carathéodory.

Développement 1.b)

Lemme 32 : Lemme de séparation d'un point et d'un convexe fermé.

Application 33 : Enveloppe convexe de $\mathrm{O}_n(\mathbb{R})$.

C/ Application en calcul différentiel. [PGCD] [OBJ]

Proposition 34 : Application différentiable de $\mathbb{R}^n$ dans $\mathbb{R}$, la différentielle est une forme linéaire et définition gradient.

Exemple 35 : La norme est différentiable sur $\mathbb{R}^n \backslash \{0\}$.

Théorème 36 : Théorème des extrema liés.

Application 37 : Théorème spectral.

Références :

— [G] Gourdon Algèbre p. 126-134

— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 441-454 et p. 681

— [OBJ] Beck, Malick Peyré Objectif Agrégation p. 20-21 et p. 97

— [ZQ] Zuily-Queffeléc p. 205

— [PGCD] Rouvière Petit Guide du Calcul Différentiel p. 43

Leçon n° 161 : Espaces vectoriels et espaces affines euclidiens : distances, isométries.

Soit $\mathcal{E}$ et $\mathcal{F}$ deux espaces affines et $\overrightarrow{E}$, $\overrightarrow{F}$ leurs sev associés.

I/ Espaces affines, euclidiens. Notion de distance.

A/ Applications affines. [AUD]

Définition 1 : Appli affine.

Remarque 2 : Ne dépend pas du choix du point de départ mais que de la partie linéaire.

Exemple 3 : Les constantes, appli linéaires, homothéties.

Proposition 4 : Composée d'applications affines.

Corollaire 5 : Groupe affine.

Proposition 6 : Isomorphisme entre groupe affine et groupe linéaire.

Lemme 7 : Lemme de structure appli affine.

Corollaire 8 : Écriture unique d'une appli affine.

Théorème 9 : Théorème de structure des appli affines.

B/ Isométries affines. [AUD]

Définition 10 : Espace affine euclidien et distance.

Définition 11 : Isométries vectorielles et affines.

Proposition 12 : $O(E)$ et $\mathrm{Isom}(E)$ sont des groupes.

Exemple 13 : Les translations, symétries orthogonales et réflexion.

C/ Distance et matrices de Gram. [G]

Définition 14 : Matrice de Gram.

Proposition 15 : Matrice de Gram $\Longleftrightarrow$ matrice hermitienne positive.

Théorème 16 : Lien distance et déterminant de Gram.

II/ Étude du groupe orthogonal.

A/ Générateurs et réduction. [PER] [AUD]

Remarque 17 : Le théorème de structure justifie cette étude.

Définition 18 : $O_n(\mathbb{R})$.

Proposition 19 : $O(\mathbb{R}^n) \simeq O_n(\mathbb{R})$ isomorphes.

Proposition 20 : $O(E)$ agit transitivement sur les bases orthonormées.

Définition 21 : $SO(E)$.

Théorème 22 : Centre de $O(E)$ et $SO(E)$.

Définition 23 : Renversements et réflexions.

Théorème 24 : $O(E)$ engendré par réflexions (et majoration nombre) et $SO(E)$ engendré par renversements (et majoration nombre).

Théorème 25 : Réduction des éléments de $O_n(\mathbb{R})$.

B/ Topologie et structure. [PER] [CAL] [OBJ] [ZQ]

Proposition 26 : Tous ces ensembles sont des sous-groupes.

Proposition 27 : $O_n(\mathbb{R})$ est compact.

Développement 1

Lemme 28 : Lemme de séparation d'un point et d'un convexe fermé.

Application 29 : Enveloppe convexe de $O_n(\mathbb{R})$.

Proposition 30 : $O_n(\mathbb{R})$ possède deux composantes connexes : $\mathrm{SO}_n(\mathbb{R})$ et $\mathrm{O}_n^-(\mathbb{R})$.

Théorème 31 : Décomposition polaire.

Application 32 : $\mathrm{GL}_n(\mathbb{R}) \overset{\text{homéo}}{\simeq} O_n(\mathbb{R}) \times \mathbb{R}^{\frac{n(n+1)}{2}}$.

C/ Conséquences sur le cas affine. [AUD]

Définition 33 : Isométries positives, déplacements.

Proposition 34 : Les éléments de $I_S(\mathcal{E})$ sont engendrés par au plus $n+1$ réflexion.

III/ Classification.

A/ Des isométries du plan. [GRIF] [AUD] [CAL]

Théorème 35 : Classification des éléments de $O_2(\mathbb{R})$.

Théorème 36 : Classification des isométries affines en dimension 2.

Proposition 37 : Les isométries du polygone régulier à n côtés est le groupe diédral D_{2n}.

B/ Des isométries de l'espace. [GRIF] [CAL]

Théorème 38 : Classification des éléments de $O_3(\mathbb{R})$.

Théorème 39 : Classification des isométries affines en dimension 3.

Développement 2

Proposition 40 : Groupe d'isométries positives du cube.

Application 41 : Colorations du cube.

Proposition 42 : Isométries du tétraèdre.

Références :

— [AUD] Audin Géométrie p. 16, p. 51-67 et p. 85
— [GRIF] Grifone Algèbre linéaire p. 395-399
— [G] Gourdon Algèbre p. 263
— [PER] Perrin Algèbre p. 141
— [CAL] Caldéro Histoires hédonistes tome 1 p. 201 et p. 360
— [OBJ] Beck, Malick Peyré Objectif Agrégation p. 97
— [ZQ] Zuily-Queffelec p. 205

Leçon n° 162 : Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.

Soit $\mathbb{K}$ un corps, n et $p \in \mathbb{N}^*$.

I/ De l'intersection d'hyperplans aux systèmes linéaires.

A/ Rencontre naturelle de systèmes linéaires. [ROM]

Théorème 1 : F de dimension r si et seulement si c'est l'intersection de $n-r$ hyperplans.

Remarque 2 : Un hyperplan = une équations à n inconnues, on a donc pour F un espace de dimension r, $n-r$ équations.

B/ Conditions d'existence et unicité des solutions. [GRIF]

Définition 3 : Système compatible et homogène.

Remarque 4 : On peut se ramener à $AX = B$ et on parle de rang du système par $\mathrm{rg}(A)$.

Exemple 5 : Exemple de système compatible et pas compatible.

Théorème 6 : Le système est compatible si et seulement si $B \in \mathrm{Im}(A)$ et S l'ensemble des solutions est un sous-espace affine dirigé par $\mathrm{Ker}(A)$ et de dimension $p - \mathrm{rg}(A)$.

Application 7 : Si $A \in \mathrm{M}_n(\mathbb{K})$ alors $\dim(\mathcal{C}(A)) \geq n$.

Définition 8 : Système de Cramer.

Proposition 9 : Une et une seule solution donnée par calcul de déterminant.

C/ Cas des matrices triangulaires. [CIA]

Proposition 10 : Méthode de la remontée en $O(n^2)$ opérations élémentaires dans le corps de base.

Remarque 11 : On cherche donc après des opérations dites élémentaires sur la matrice à se ramener à une matrice triangulaire et utiliser la méthode de la remontée.

II/ Résolution pratique d'un système linéaire.

A/ Algorithme du pivot de Gauss. [OBJ] [GRIF] [CAL]

Proposition 12 : L'ensemble des solutions ne change pas après opérations élémentaires sur A.

Définition 13 : Matrices de transvection, dilatation, transposition.

Proposition 14 : Multiplication à gauche = agir sur les lignes, multiplication à droite = agir sur les colonnes.

Définition 15 : Matrice échelonnée en ligne.

Exemple 16 : Exemple de telle matrice.

Définition 17 : Action par translation à gauche $(P, A) \mapsto PA$.

Théorème 18 : Action sur les lignes et on a toujours une forme échelonnée réduite dans une orbite.

Application 19 : Algo de pivot de Gauss => se ramener à échelonnée réduite par opérations élémentaires.

Exemple 20 : Exemple de passage de matrice à échelonnée réduite.

Remarque 21 : $\mathrm{rg}(A)$ pivots donc le reste donne les conditions de compatibilité.

Application 22 : Calcul en $O(n^3)$ opérations élémentaires de $\mathrm{rg}(A)$, $\mathrm{Ker}(A)$, $\mathrm{Im}(A)$, $\det(A)$ et A^{-1}.

B/ Factorisation LU. [ROM] [CIA]

Proposition 23 : Factorisation LU.

Application 24 : $O(n^3)$ opérations pour n systèmes linéaires avec même matrice A au lieu de $O(n^4)$ opérations pour le pivot de Gauss.

C/ Applications du pivot de Gauss. [ROM] [GRIF] [FGNAlg2]

Développement 1

Théorème 25 : Ici, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, Générateurs de $\mathrm{SL}_n(\mathbb{K})$ et $\mathrm{GL}_n(\mathbb{K})$.

Application 26 : $\mathrm{GL}_n(\mathbb{R})$ a deux composantes connexes $\mathrm{GL}_n^+(\mathbb{R})$ et $\mathrm{GL}_n^-(\mathbb{R})$ et $\mathrm{SL}_n(\mathbb{K})$ est connexe par arcs.

Application 27 : Déterminer si une famille est libre.

Application 28 : Déterminer les équations vérifiant un sev.

Application 29 : Vérifier si un vecteur $v \in \mathrm{Vect}(v_1, \ldots, v_p)$.

Application 30 : Vérifier si $\{v_1, \ldots, v_p\}$ est génératrice.

Application 31 : Déterminer une base de $F \cap G$ et $F + G$ à partir d'une base de F et d'une base de G.

D/ Le cas d'un anneau A euclidien. [OBJ]

Développement 2

Proposition 32 : Forme normale de Smith : existence et unicité.

Remarque 33 : Variante du pivot sur $\mathbb{Z}$.

Application 34 : Théorème de structure des groupes abéliens finis.

III/ Résolution numérique de systèmes par méthode itérative. [ALL]

Définition 35 : Méthode itérative qui converge.

Proposition 36 : Méthode itérative converge si et seulement si $\rho(M^{-1}N) < 1$.

Définition 37 : Méthode de Jacobi et Gauss-Seidel.

Proposition 38 : Convergence des deux méthodes si A est à diagonale fortement dominante.

Références :

— [ROM] Rombaldi p. 451
— [GRIF] Grifone Algèbre linéaire p. 141-148
— [CIA] Ciarlet Introduction à l'analyse numérique matricielle p. 82-90
— [CAL] Caldéro Nouvelles Histoires Hédonistes tome 1 p. 203, p. 213
— [FGNAlg2] Francinou Gianella Nicolas Algèbre 2 p. 177
— [ALL] Allaire Analyse numérique p. 428
— [OBJ] Beck Malick Peyré Objectif Agrégation p. 186, p. 285

Leçon n° 170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité. Applications.

Soit $\mathbb{K}$ un corps de caractéristique différente de 2, E un $\mathbb{K}$-ev de dimension $n \geq 1$.

I/ Généralités sur les formes quadratiques.

A/ Formes bilinéaires et formes quadratiques. [ROM] [GRIF] [G]

Définition 1 : Forme bilinéaire symétrique.

Définition 2 : Matrice d'une forme bilinéaire + expression dans une base.

Définition 3 : Forme quadratique et forme polaire.

Proposition 4 : Unicité forme polaire et formule de polarisation.

Remarque 5 : Forme quadratique est un polynôme homogène de degré 2.

Proposition 6 : Isomorphisme entre $Q(E)$ et $S_2(E)$ et donc dimension de $Q(E)$.

Exemple 7 : Exemple de forme quadratique.

Remarque 8 : Vision matricielle des formes quadratiques.

Proposition 9 : On fait agir $\mathrm{GL}_n(\mathbb{K})$ sur $S_n(\mathbb{K})$ par congruence, les orbites représentent les même formes quadratiques mais dans des bases différentes et elles sont dites congruentes.

Définition 10 : Discriminant défini à multiplication par un carré près.

Proposition 11 : Deux matrices congruentes ont donc même discriminant.

B/ Orthogonalité, rang, isotropie. [ROM]

Définition 12 : Deux éléments orthogonaux et orthogonal d'une partie.

Théorème 13 : Les différentes propriétés sur les orthogonaux.

Définition 14 : Définition vecteur isotrope et cône isotrope.

Exemple 15 : Cônes isotropes de $q(x,y) = x^2 - y^2$ et $q(x,y,z) = x^2 + y^2 - z^2 +$ annexe.

Définition 16 : Noyau de q.

Proposition 17 : $\mathrm{Ker}(q) \subset C_q$.

Définition 18 : Forme quadratique non dégénérée et définie.

Définition 19 : Rang d'une forme quadratique.

Développement 1.a)

Théorème 20 : Somme directe $F \oplus F^{\perp} = E$ si et seulement si $q|_F$ est non dégénérée.

Définition 21 : Base q-orthogonale.

Théorème 22 : Existence d'une base q-orthogonale.

II/ Réduction et classifications des formes quadratiques.

A/ Réduction de Gauss. [ROM] [G] [GRIF]

Théorème 23 : Réduction de Gauss.

Corollaire 24 : Forme polaire après réduction.

Corollaire 25 : Existence de base rendant q diagonale.

Définition 26 : Formes quad positives et négatives (définies).

Proposition 27 : Cauchy-Schwarz.

Proposition 28 : Égalité noyau et cône isotrope si positive.

B/ Classification sur $\mathbb{R}$. [GRIF] [G]

Théorème 29 : Inertie de Sylvester et signature.

Corollaire 30 : Lien positivité et signature.

Exemple 31 : Donner un exemple de forme quadratique réelle et lien avec sa signature.

Proposition 32 : Deux formes quadratiques réelles sont congruentes si elles ont même signature.

Remarque 33 : On a donc $r+1$ classes d'équivalences pour les formes quadratiques de rang r.

Développement 1.b)

Application 34 : Critère de Sylvester.

C/ Classification sur $\mathbb{C}$. [GRIF]

Théorème 35 : Classification sur $\mathbb{C}$.

Remarque 36 : Il y a donc 1 classe d'équivalence pour les formes quadratiques de rang donné et $n+1$ classes d'équivalences en tout.

D/ Classification sur $\mathbb{F}_q$. [ROM]

Proposition 37 : Nombres de carrés de $\mathbb{F}_q$.

Théorème 38 : Classification sur $\mathbb{F}_q$.

Corollaire 39 : Congruentes si et seulement si le rapport de discriminant est un carré + classes d'équivalences.

Définition 40 : Symbole de Legendre.

Développement 2

Application 41 : Loi de réciprocité quadratique.

Remarque 42 : Permet de déterminer avec le calcul des symboles de Legendre si deux formes quadratiques sont congruentes.

Références :

— [G] Gourdon Algèbre p. 227-240

— [GRIF] Grifone Algèbre linéaire p. 295-309

— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 461-483

Leçon n° 181 : Convexité dans $\mathbb{R}^n$. Applications en algèbre et en géométrie.

Soit E un $\mathbb{R}$-ev de dimensions $n \geq 1$. X un espace affine de direction E.

I/ Ensembles et fonctions convexes.

A/ Barycentres. [AUD] [TAU]

Définition 1 : Barycentre.

Notation 2 : Notation barycentre.

Proposition 3 : Associativité Barycentre.

Application 4 : Concours des médianes d'un triangle.

Définition 5 : Isobarycentre.

Application 6 : Suites de polygone + annexe.

B/ Parties convexes d'un espace affine réel. [TAU]

Définition 7 : Segment fermé et ouvert.

Définition 8 : C est convexe si et seulement si tout segment reste dans C.

Exemple 9 : Les convexes de $\mathbb{R}$ sont les intervalles.

Exemple 10 : Les boules sont convexes.

Définition 11 : Combinaison convexe.

Proposition 12 : C convexe ssi tte combinaison convexe de points de C reste dans C.

Proposition 13 : Un convexe est connexe par arcs.

Exemple 14 : Les sous-espaces affines/vectoriels sont convexes.

Proposition 15 : L'image directe et réciproque d'un convexe par une application affine est convexe.

Application 16 : Les demi-espaces sont convexes.

Proposition 17 : Une intersection quelconque de convexes reste convexe.

C/ Fonctions convexes. [ROM]

Définition 18 : Fonctions convexes sur un ensemble convexe.

Proposition 19 : f convexe si et seulement si son épigraphe est convexe + annexe.

Proposition 20 : f convexe si et seulement si $f'' \geq 0$.

Exemple 21 : Γ est convexe.

Proposition 22 : det est log-convexe sur $S_n^{++}(\mathbb{R})$.

Application 23 : Inégalité de Hölder.

Proposition 24 : Inégalité de Jensen.

II/ Propriétés topologiques des ensembles convexes.

A/ Enveloppe convexe. [TAU] [FGNAlg1]

Définition 25 : Enveloppe convexe.

Proposition 26 : L'enveloppe convexe est l'ensemble des combinaisons convexes d'éléments de la partie.

Algorithme 27 : Algorithme de Graham pour trouver l'enveloppe convexe d'un nombre fini de points + annexe.

Développement 1

Théorème 28 : Gauss-Lucas.

Proposition 29 : Son énoncé équivalent.

Application 30 : Application à un polynôme

Proposition 31 : Si A ouverte alors $\mathrm{Conv}(A)$ est ouverte.

Théorème 32 : Carathéodory.

B/ Compacité. [TAU] [ZQ]

Proposition 33 : Si A compacte alors $\mathrm{Conv}(A)$ compacte.

Développement 2.a)

Application 34 : Enveloppe convexe de $\mathrm{O}_n(\mathbb{R})$.

Proposition 35 : Si A bornée, $\mathrm{Conv}(A)$ aussi et les diamètres sont égaux.

C/ Intérieur et adhérence. [TAU]

Proposition 36 : Si A convexe alors $\overline{A}$ convexe et $\mathring{A}$ est convexe + props.

Proposition 37 : Si A convexe alors $\mathring{A} \neq \emptyset \iff A$ contient $n+1$ points affinements indépendants $\iff \langle A \rangle = X$.

D/ Hyperplans de séparation. [OBJ] [TAU]

Définition 38 : Hyperplan de séparation.

Théorème 39 : Projection sur un convexe fermé.

Développement 2.b)

Application 40 : Existence hyperplan de séparation séparant un point d'un convexe fermé.

E/ Points extrémaux. [TAU]

Définition 41 : Point extrémal.

Proposition 42 : Propriétés équivalentes.

Théorème 43 : Krein-Millman.

Références :

— [AUD] Audin Géométrie p. 29
— [TAU] Tauvel Géométrie p. 17 et p. 69-83
— [ROM] Rombaldi Éléments d'analyse réelle p. 225-245
— [FGNAlg1] Francinou, Gianella, Nicolas Algèbre tome 1 p. 229
— [OBJ] Beck, Malick Peyré Objectif Agrégation p. 97
— [ZQ] Zuily-Queffeléc p. 205

Leçon n°190 : Méthodes combinatoires, problèmes de dénombrement.

Dans toute la suite on notera E et F deux ensembles.

I/Dénombrement.

A/ Les ensembles finis. [G] [G Analyse]

Définition 1 : Equipotence et cardinal.

Théorème 2 : Equipotents si et seulement si les ensembles ont mêmes cardinaux.

Proposition 3 : Si $F \subset E$ alors $|F| \leq |E|$ et cas d'égalité.

Corollaire 4 : Principe des tiroirs.

Application 5 : Tout irrationnel est proche d'un rationnel.

B/ Principe additif. [G]

Proposition 6 : Cardinal union disjointe.

Corollaire 7 : Lemme des bergers.

Corollaire 8 : Cardinal différence.

Théorème 9 : Crible de Poincaré pour 2 et n ensembles.

C/ Principe multiplicatif. [G]

Proposition 10 : Cardinal produit cartésien.

Corollaire 11 : Cardinal applications.

Corollaire 12 : Cardinal parties d'un ensemble.

Définition 13 : k-listes et k arrangements noté A_k^n.

Proposition 14 : Valeur de A_k^n.

Exemple 15 : Interprétation de cette valeur en terme de remise de boule.

Proposition 16 : Nombre d'injections.

Corollaire 17 : Cardinal $\mathfrak{S}(E)$.

D/ Combinaison. [G]

Définition 18 : Coefficient binomial.

Proposition 19 : Propriétés de ce coefficient (Pascal).

Exemple 20 : Nombres de surjections, $n = \sum_{d|n} \varphi(d)$.

Proposition 21 : Binôme de Newton, multinôme et formule de Vandermonde.

E/ Séries génératrices. [G]

Définition 22 : Série génératrice et série exponentielle.

Remarque 23 : Unicité série formelle permet d'obtenir des relations.

Exemple 24 : Nombre de dérangements, nombres de Bell.

II/ Formules d'inversion.

A/ Inversion de Pascal. [ROM]

Théorème 25 : Inversion de Pascal.

Corollaire 26 : Nombre de surjections.

B/ Inversion de Möbius. [ROM]

Définition 27 : Fonction de Möbius.

Développement 1

Lemme 28 : Calcul de $\sum_{d|n} \mu(d)$.

Théorème 29 : Inversion de Möbius.

Théorème 30 : $X^{p^n} - X = \prod_{d|n} \prod_{P \in U_n(p)} P$ et dénombrement des polynômes irréductibles de degré donné avec équivalent.

Application 31 : Probabilité que deux nombres soient premiers entre eux.

III/ Groupes et combinatoire.

A/ Actions de groupes. [PER] [CAL]

Théorème 32 : Lagrange.

Proposition 33 : Si morphisme lien entre les cardinaux de l'image et du noyau.

Définition 34 : Action de groupe. Et définition équivalente se donner un morphisme.

Définition 35 : Orbite et stabilisateur.

Proposition 36 : $|G| = |w(x)||\mathrm{Stab}(x)|$.

Théorème 37 : Équation aux classes.

Application 38 : Dénombrement des endomorphismes diagonalisables de $\mathbb{F}_q^n$.

Théorème 39 : Formule de Burnside.

Développement 2

Application 40 : Isométries du cube et colorations.

Application 41 : Problème de la roulette.

B/ Isomorphismes exceptionnels. [CAL]

Définition 42 : Définition groupes projectifs linéaires.

Proposition 43 : Dénombrement sur les corps finis : $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathbb{P}^n(F_q)$, $\mathrm{SL}_n(\mathbb{F}_q)$, $\mathrm{PGL}_n(\mathbb{F}_q)$ et $\mathrm{PSL}_n(\mathbb{F}_q)$.

Lemme 44 : Si H est un sous-groupe d'indice n de $\mathfrak{S}_n$ alors $H \simeq \mathfrak{S}_{n-1}$.

Théorème 45 : Isomorphismes exceptionnels.

Références :

— [G] Gourdon Algèbre 3ème éd. p. 299-312, p. 312, p. 314
— [G Analyse] Gourdon Analyse p. 275
— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 51 et p. 331 et p. 423
— [CAL] Caldéro Histoires hédonistes tome 1 p. 250, p. 264 et p. 363
— [PER] Perrin Algèbre p. 13

Leçon n° 191 : Exemples d'utilisation des techniques d'algèbre en géométrie.

I/ Utilisation de l'algèbre linéaire en géométrie.

A/ Déterminant : interprétation du volume. [OBJ] [G] [ROM] [FGNAlg3]

Théorème 1 : Déterminant et mesure de Lebesgue.

Application 2 : Volume parallélépipède.

Application 3 : Inégalité de Hadamard et interprétation géométrique.

Application 4 : Volume d'un ellipsoïde et ellipsoïde de John-Loewner.

Définition 5 : Matrice de Gram.

Proposition 6 : Toute matrice hermitienne définie positive est une matrice de Gram. Réciproque vraie.

Théorème 7 : Distance à un sev.

Proposition 8 : Orientation d'un espace euclidien : relation d'équivalence.

Définition 9 : Se donner une orientation = se donner une classe d'équivalence.

Proposition 10 : u isométrie positive si et seulement si transforme BON en BON avec même orientation.

Application 11 : La symétrie centrale par rapport à l'origine est négative car transforme une BON directe en BON indirecte.

B/ Une application sur l'approche d'isobarycentre. [G]

Définition 12 : Isobarycentre de complexes.

Lemme 13 : Déterminant circulant.

Application 14 : Suite de polygones + annexe.

C/ Utilisation du résultant en géométrie. [SP]

Définition 15 : Résultant dans un anneau intègre.

Proposition 16 : Propriétés de calcul.

Proposition 17 : Dans le corps de fractions $P \wedge Q = 1 \iff \mathrm{Res}(P,Q) \neq 0$.

Lemme 18 : Lemme de spécialisation.

Théorème 19 : Dans $\mathbb{K}$ algébriquement clos alors si le résultant est nul on peut remonter à une solution globale d'un système polynomial

Application 20 : Méthode d'élimination des variables pour un système donné.

Application 21 : Autre système (ex intersection sphère et plan) + annexe.

Application 22 : Paramétrisation rationnelle du cercle.

II/ Utilisation de la théorie des groupes en géométrie.

A/ Action de groupe. [PER]

Définition 23 : Action.

Définition 24 : Orbites et stabilisateur.

Remarque 25 : Les actions ont un lien fort avec la géométrie : on peut agir sur une structure géométrique.

Définition 26 : Action fidèle.

Application 27 : Théorème de Cayley.

Théorème 28 : Équation aux classes.

Théorème 29 : Formule de Burnside.

Application 30 : Coloration des colliers + annexe.

B/ Application aux isométries laissant stable des polytopes. [CAL]

Définition 31 : $I_S(X)$ et $I_S^+(X)$.

Proposition 32 : Le groupe diédral D_{2n} est le groupe des isométries du polygone régulier à n côtés.

Proposition 33 : Isométries du triangle équilatéral + annexe.

Développement 1

Théorème 34 : Isométries du cube + annexe.

Application 35 : Colorations du cube.

Proposition 36 : Isométries du tétraèdre régulier.

III/ Utilisation de la théorie des corps en géométrie.

A/ Premières propriétés. [CAR]

Définition 37 : Nombres constructibles.

Proposition 38 : Perpendiculaire, parallèle, milieu, médiane, bissectrice + annexe.

B/ Lien avec la théorie des corps. [CAR]

Théorème 39 : L'ensemble $\mathcal{C}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

Lemme 40 : Équations cartésiennes pour droites et cercles.

Développement 2.a)

Théorème 41 : Théorème de Wantzel.

Corollaire 42 : Résultat de Wantzel.

C/ Réponse aux trois problèmes historiques. [CAR]

Corollaire 43 : La quadrature du cercle est impossible.

Développement 2.b)

Corollaire 44 : La duplication du cube est impossible.

Corollaire 45 : La trissection de l'angle est impossible en général.

Références :

— [PER] Perrin Algèbre p. 13
— [G] Gourdon Algèbre p. 146 et p. 263
— [ROM] Rombaldi Algèbre et géométrie 2nd éd. p. 563
— [FGNAlg3] Francinou, Gianella Nicolas Algèbre 3 p. 229
— [SP] Saux-Picart Cours de calcul formel tome 1 p. 143-150
— [OBJ] Beck Malick Peyré Objectif Agrégation p. 184
— [CAR] Carréga Théorie des corps p. 13-37
— [CAL] Caldéro Histoires hédonistes tome 1 p. 363