101 - Groupe opérant sur un ensemble. Exemples et applications.

Références [AB], [Com98], [MT86], [Per96].

I Propriétés des actions de groupes

• I.A Définitions

Définition I.1. Soit G un groupe et X un ensemble. Une *action* de G sur X est un morphisme de groupe $G \to Bij(X)$. L'action de $g \in G$ sur $x \in X$ sera noté $g.x$.

Exemple I.2. $\mathfrak{S}_n$ agit sur $K[X_1, ..., X_n]$ par permutation des indéterminées. Les polynômes symétriques sont les polynômes invariant par $\mathfrak{S}_n$ et les polynômes antisymétriques sont les polynômes P tels que $\sigma.P = \det(\sigma)P$.

Définition I.3. Une action est *fidèle*, si l'applications $G \to Bij(X)$ est injective. L'action est dite transitive si : $\forall x, y \in X, \forall g \in G, g.x = y$. Une action est k-transitive si $(x_1, ..., x_k)$ distincts et $(y_1, ..., y_k)$ distinct il exsite $g \in G$ tel que $g.x_i = y_i$ $(i \leq k)$.

Exemple I.4.
- L'action de $\mathfrak{A}_n$ sur $[1, n]$ est $(n-2)$-transitive.
- Le groupe $PGL_3(\mathbb{R})$ agit de façon 3-transitive sur $P^2(\mathbb{R})$.
- Le groupe des isométries d'un polyèdre régulier agit simplement transitivement sur ses drapeaux.
- Soit $P(X) \in Q[X]$, alors son groupe de Galois agit de façon transitive sur ses racines si et seulement si $P(X)$ est irréductibles. Et il agit par permutation paire si et seulement son discriminant est un carré dans $\mathbb{Q}$.

Proposition I.5. $G/\ker\rho \to Bij(X)$ est une action fidèle.

Exemple I.6.
- G agit par lui même par conjuguaison et induit un isomorphsime $Int(G) \cong G/Z(G)$.
- Le groupe $PGL_n(\mathbb{R})$ agit de façon fidèle sur $P^{n-1}(\mathbb{R})$.
- Développement La sphère S^3_H des quaternions induit un isomophisme $PSU_2(\mathbb{C}) \simeq SO_3(\mathbb{R})$.

• I.B Orbites et stabilisateurs

Définition I.7.
- L'*orbite* de $x \in X$ par G est $Orb_G(x) = G.x = \{g.x | g \in G\}$.
- Le *stabilisateur* de x est $Stab_G(x) = \{g \in G | g.x = x\}$.
- Le *fixateur* de $g \in G$ est $Fix_X(g) = \{x \in X | g.x = x\}$.

Exemple I.8.
- Action par conjuguaison : le stabilisateur de 1 est le centre et les orbites sont les classes de conjuguaisons.
- Le groupe $GL_n(A) \times GL_n(A)$ agit sur $\mathcal{M}_n(A)$ par équivalences. Ses orbites sont déterminées par les diviseur élémentaires.

Proposition I.9.
- Si $y = g.x$, alors $Orb_G(y) = Orb_G(x)$. L'ensemble des orbites forme une partition de X.
- Si $y = g.x$, alors $Stab_G(y) = gStab_G(x)g^{-1}$.

Applications I.10. Si $\sigma \in \mathfrak{S}_n$, les orbites de $Gr(\sigma)$ sur $[1, n]$ donnent la décomposition en cycles à supports disjoints de σ.

Proposition I.11. On a une bijection $G/Stab_G(x) \to Orb_G(x)$.

Exemple I.12. Si $H \subset G$ alors G agit transitivement sur G/H. On a $Stab(gH) = gHg^{-1}$. De plus $\ker\rho = \bigcap_{g\in G} gHg^{-1}$.

Applications I.13 (Théorème de Frobénius)**.** Si p est le plus petit nombre premier divisant $\sharp G$, alors tout sous groupe H d'indice H est distingué.

II Actions de groupes finis

• II.A Formules de dénombrement

Proposition II.1. Pour tout $x \in X$, on a $\sharp Orb_G(x).\sharp Stab_G(x) = \sharp G$.

Théorème II.2. Si $(x_1, \ldots, x_p)$ est un système de représentant des orbites, alors $\sharp X = \sum_{i=1}^{p} \sharp Orb_G(x_i)$.

Applications II.3. L'action par conjugaison donne l'équation des classes

$$\sharp G = Z(G) + \sum_{Cl(x_i)\neq Cl(1)} \sharp Orb_G(x_i).$$

Donc le centre d'un p-groupe est non trivial.

Corollaire II.4. Si g est un p-groupe, alors $\sharp \bigcap_{g\in G} Fix(g) = \sharp X \mod p$.

Applications II.5. Développement Théorème de Wedderburn : tout corps fini est commutatif.

Théorème II.6 (Formule de Burnside)**.** $\sharp G \sharp Orbites = \sum_{g\in G} \sharp Fix_X(g)$.

Applications II.7. Développements Dénombrement des coliers de perles et dénombrement des coloriages du cube.

• II.B Applications l'étude des groupes finis

Théorème II.8 (Théorème de Cauchy)**.** Soit p premier, si $p|\sharp G$, alors G contient un élément d'orde p.

Corollaire II.9. $\mathbb{Z}/p\mathbb{Z}$ est le seul groupe d'ordre p.

Théorème II.10 (Théorème de Calay)**.** Tout groupe fini s'injecte dans $\mathfrak{S}_{\sharp G}$.

Proposition II.11. Le centre d'un p-groupe est non trivial.

Théorème II.12. Développement [Sylow] Tout groupe fini admet un p-Sylow. De plus tous les p-Sylow sont conjugués et le nombre de p-Sylw est congrue à 1 mod p et divive $\sharp G$.

Applications II.13. L'action de G sur ses Sylows permet de démontrer les choses suivantes

- Tout sous-groupe d'ordre < 60 n'est pas simple ou est trivialement simple.
- Développement Le groupe $\mathfrak{A}_5$ est le seul sous-groupe d'ordre 60.

III Action du groupe matricielle

• III.A Action de $O_n(\mathbb{R})$ en géométrie

Action sur les formes quadratiques $GL_n(\mathbb{R})$ agit à droite sur $Q(\mathbb{R}^n)$ par composition.

Théorème III.1. Développement [Sous-groupe compacts] Si G est un sous-groupe compact de $GL_n(\mathbb{R})$, alors G fixe un produit scalaire.

Action du groupe des rotations L'action de $SO_2(\mathbb{R})$ sur $\mathbb{S}^1$ est simplement transitive. L'angle entre deux vecteurs unitaires u, v est l'unique $\theta \in \mathbb{R}/Z$ tel que $R_\theta = u, v$.

Duplication de la sphère

Définition III.2. Le *groupe libre* de rang 2, noté F_2, est l'ensemble des mots sur $\{a, a^{-1}, b, b^{-1}\}$, munie de la concaténation avec ε le mot vide et la règle $aa^{-1} = a^{-1}a = bb^{-1} = b^{-1}b = \varepsilon$. Tout éléments de F_2 s'écrit de façon unique sous la forme $a^{\alpha_1}b^{\beta_1}\dots a^{\alpha_p}b^{\beta_p}$, avec $\alpha_i, \beta_i \in \mathbb{Z}^*$ et $\alpha_1, \beta_p \in \mathbb{Z}$.

Théorème III.3. Développement [Banach-Tarski faible] Il existe :

- D une partie dénombrable au plus de $\mathbb{S}^2$.
- Une partition de $\mathbb{S} \setminus D$ en 4 partie : $\mathbb{S} \setminus D = A_1 \sqcup A_2 \sqcup A_3 \sqcup A_4$
- Deux rotations $f, g \in SO_3(\mathbb{R})$. Tels que
$$\mathbb{S}^2 \setminus D = A_1 \sqcup a(A_2) = A_3 \sqcup b(A_4).$$

Groupes des isométries des polyèdres

Théorème III.4.
- Le groupe des isométries du tétraèdre est isomorphe à $\mathfrak{A}_4$.
- Le groupe des isométries du cubde est isomorphe à $\mathfrak{S}_4$.
- Développement Le groupe des isométries du dodécaèdre est isomorphe à $\mathfrak{A}_5$.

Théorème III.5. Développement Les sous-groupes finis de $SO_3(\mathbb{R})$: sont isomorphes à : $\mathbb{Z}/n\mathbb{Z}/$, D_{2n}, $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$. De plus si deux sous-groupes sont isomorphes, alors ils sont conjugués.

• III.B Action du groupe modulaire

Le *groupe modulaire* $SL_2(\mathbb{Z})$ agit sur $\mathcal{H}$ par homographie : pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ et $z \in \mathcal{H}$, l'action es donnée par : $\gamma.z = \dfrac{az+b}{cz+d}$.

On note $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Proposition III.6. Le groupe modulaire est engendré par S, T.

Proposition III.7. Un domaine fondamental est donné par $\{z \in \mathcal{H} \mid Re(z) \in [-1/2, 1/2], |z| \geq 1\}$.

Définition III.8. Un *réseau* de $\mathbb{C}$ ou *tore complexe* est un sous-groupe du type $\Lambda = \mathbb{Z}u \oplus \mathbb{Z}v$, avec u, v deux vecteurs libres sur $\mathbb{R}$. Deux réseaux Λ_1, Λ_2 sont dit isomorphes s'il existe $a \in \mathbb{C}$ tel que $a\Lambda_1 = \Lambda_2$.

Théorème III.9. Développement On note R l'ensemble des réseaux modulo isomorphismes. Alors l'application suivante est une bijection

$$\begin{array}{ccc} \mathcal{H}/SL_2(\mathbb{Z}) & \longrightarrow & R \\ \tau \mod SL_2(\mathbb{Z}) & \longmapsto & \mathbb{Z} \oplus \mathbb{Z}\tau \end{array}.$$

IV Développements

- Théorème de Banach-Tarski.
- Groupe des polyèdres.
- Sous-groupes finis de $SO_3(\mathbb{R})$.
- Action du groupe modulaire.
- Théorème de Sylow.
- Simplicité de $\mathfrak{A}_n$.
- Automorphismes de $\mathfrak{S}_n$.
- Théorème de Wedderburn.
- Groupe des paveurs.
- Coloriages du cube et colliers de perles.
- $PSL_2(\mathbb{R}) \simeq O_0(2,1)$.
- $PSU_2(\mathbb{C}) \simeq SO_3(\mathbb{R})$.

103 - Exemples et applications des notions de sous-groupe distingué et de groupe quotient

Références [...]

I Sous-groupes distingués

• I.A Définitions et propriétés

Définition I.1. Un sous-groupe H de G est *distingué* s'il est stable par conjugaison. On note alors $H \triangleleft G$.

Exemple I.2.
- Tout sous-groupe d'un groupe abélien est distingué.
- Le centre d'un groupe est distingué.
- Le groupe des quaternions est non-abélien mais tous ses sous-groupes sont distingués.

Proposition I.3. Le noyau d'un morphisme de groupe est distingué.

Exemple I.4.
- $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$.
- Si G admet un unique p-Sylow, alors il est distingué (par théorème de Sylow).

Proposition I.5. Si l'indice de H est le plus petit facteur premier divisant G, alors H est distingué.

• I.B Groupes quotients

Proposition I.6. Si $H \triangleleft G$, alors G/H est muni de la loi de groupe : $xH.yH = xyH$. De plus si G est fini, alors $\operatorname{Card} G/H = (\operatorname{Card} G)/(\operatorname{Card} H)$.

Exemple I.7.
- $\mathbb{Z}/N\mathbb{Z}$.
- ???

Proposition I.8. Si $f : G \to K$ est un morphisme de groupe, alors f induit un isomorphisme $\operatorname{Im} f \cong G/\ker f$.

• I.C Simplicité

Définition I.9. Un groupe est *simple* s'il n'a pas de sous-groupe distingué stricte.

Proposition I.10. Si G est simple, alors tout morphisme de G vers H est soit injectif soit trivial.

Exemple I.11.
- $\mathbb{Z}/p\mathbb{Z}$ est simple pour p premier.
- Tout groupe d'ordre < 60 est soit $\mathbb{Z}/p\mathbb{Z}$ soit non simple.

Exemple I.12.
- Développement $\mathfrak{A}_n$ est simple pour $n \geq 5$.
- $PSL_n(k)$ est simple sauf pour $(n,k) = (2,2)$ et $(2,3)$.
- $SO_3(\mathbb{R})$ est simple.

Applications I.13. Si H est un sous-groupe de $\mathfrak{S}_n$ d'indice n, alors H est isomorphe a $\mathfrak{S}_n$. Si de plus $n \neq 6$, alors il existe $k \in [1,n]$ tel que $H = Stab(k)$.

Proposition I.14. Développement Le groupe $\mathbb{A}_5$ est est le seul groupe simple d'ordre 60.

• I.D Groupe-dérivé, abélianisé et résolubilité

Définition I.15.
- Soit G un groupe et $x, y \in G$. Le *commutateur* de x et de y est $[x,y] = xyx^{-1}y^{-1}$. Le *groupe dérivé* $D(G)$ de G est le sous-groupe engendré par les commutateurs.
- Soit H un sous-groupe de G. Le *normalisateur* est $N_H(G) = \{x \in G : xHx^{-1} = H\}$.

Exemple I.16.
- $D(GL_n(\mathbb{R})) = SL_n(\mathbb{R})$.
- $D(\mathfrak{S}_n) = \mathfrak{A}_n$

Proposition I.17.
- $D(G) = \{1\}$ si et seulement si G est abélien.
- Le groupe $D(G)$ est distingué et c'est le plus petit sous-groupe distingué de G dont le quotient est abélien.
- Soit H groupe abélien et $f : G \to H$ un morphisme de groupe. Alors f se factorise dans $G/D(G)$.

Définition I.18. L'*abélianisé* de G est $G^{ab} = G/D(G)$.

Proposition I.19. Si H est commutatif et si $f : G \to H$ est un morphisme de groupe, alors f se quotiente dans G^{ab}.

Applications I.20 (Théorème de Frobénius-Zolotarev)**.** Soit $p \geq 3$ premier et $M \in \mathcal{M}_n(\mathbb{F}_p)$. Alors $\varepsilon M = \left(\frac{\det M}{p}\right)$.

Définition I.21. Un groupe G est *résoluble* si la suite $G \supset D(G) \supset D^2(G) \supset \cdots$ stationne à 1.

Exemple I.22.
- $\mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \{1\}$.
- $\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset V_4 \supset \{1\}$.
- Pour $n \geq 5$, $\mathfrak{S}_n \supset \mathfrak{A}_n$.

Théorème I.23. Développement [Lie-Kolchin] Si G est un groupe connexe résoluble de $GL_n(\mathbb{C})$. Alors G est trigonalisable.

Théorème I.24 (Correspondance de Galois)**.** Soit L/K une extension Galoisienne et G son groupe de Galois. Alors :
- On a une bijection entre {sous-groupes de G} et {sous-extension de L}.
- On a une suite exacte :

$$1 \longrightarrow H \longrightarrow N_H(G) \longrightarrow Aut(K^H, K) \longrightarrow 1.$$

– L'extension K^H/K est Galoisienne si et seulement si H est distingué dans G.

Théorème I.25. Un polynôme est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.

II Produit semi-direct de groupes

• II.A Produit semi-directe de sous-groupes

Théorème II.1. Soient H, K deux sous-groupes de G tel que :
– H est stable par conjugaison par K.
– $H \cap K = \{1\}$.

Alors
– $HK = \{hk \mid h \in H, k \in K\}$ est un sous-groupe de G et $HK = KH$.
– L'application $f : H \times K \to HK$ est bijective et on a : $f(h,k).f(h',k') = f(h.kh'k^{-1}, kk')$.

Définition II.2. Si H, K vérifient les hypothèses du théorème, alors le produit semi-direct $H \rtimes K$ est le produit $H \times K$ muni de la loi de groupe $(h,k) * (h',k') = (hkh'k^{-1}, kk')$.

Si $HK = G$ alors G est isomorphe au produit semi-direct $H \rtimes K$.

Exemple II.3.
– Produit directe : $G \times H = (G \times \{1\}) \rtimes (\{1\} \times H) = (\{1\} \times H) \rtimes (G \times \{1\})$.
– Groupe affine : E est un espace affine et $O \in E$, alors $GA(E) = T \rtimes Fix(O)$, où T est le sous-groupe des translations.

• II.B Produit semi-directe de groupes quelconques

Définition II.4. Soient H, K deux groupes et $\phi : K \to Aut(H)$ une action de K sur H. Le produit semi directe $H \rtimes_\phi K$ est le groupe $H \times K$ munie de la loi $(h,k) * (h',k') = (h.\phi_k(h'), kk')$.

Proposition II.5. Le produit semi-directe est abélien si et seulement si l'action est triviale.

Exemple II.6.
– $\mathfrak{S}_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rtimes \mathfrak{S}_3$.
– $D_{2n} = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. (Dans ls deux cas il n'y a qu'un seul produit semi-directe non directe à isomorphisme près).

Proposition II.7. Soit une suite exacte :

$$1 \to H \to G \xrightarrow{p} K \to 1.$$

Si p admet une section q d'image K', alors $G = H \rtimes K' = H \rtimes_\phi K'$, avec $\phi(k).h = q(k)hq(k)^{-1}$

Proposition II.8. Soient G, H deux groupes et $\phi, \psi : G \to Aut(H)$.
– S'il existe $\alpha \in Aut(G)$ tel que $\psi = \phi \circ \alpha$, alors $H \rtimes_\phi G$ et $H \rtimes_\psi G$ sont isomorphes.
– S'il existe $x \in H$ tel que $\psi = int_x \circ \phi$, alors $H \rtimes_\phi G$ et $H \rtimes_\psi G$ sont isomorphes.

Applications II.9.
– A conjugaison près, il existe 3 morphismes de $\mathfrak{S}_4$ vers $\mathfrak{S}_3$.
– Développement Soient $p < q$ deux nombres premiers. Si $p \nmid q-1$, alors $\mathbb{Z}/pq\mathbb{Z}$ est le seul groupe d'ordre pq, et si $p|q$ il y a en plus $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$..
– Développement Les groupes d'ordre 12 sont : $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \rtimes V_4$, $V_2 \rtimes \mathbb{Z}/3\mathbb{Z}$.

Remarque II.10. Si un groupe est simple, alors on ne peut pas le dévisser.

III Développements

– $\mathfrak{A}_5$ est le seul groupe simple d'ordre 60.
– Théorème de Lie-Kolchin.
– Groupes d'ordre 12 et d'ordre pq.
– Simplicité de $\mathfrak{A}_n$.
– Simplicité de SO_3.
– Simplicité de $PSL_n(k)$.
– Automorphismes de $\mathfrak{S}_n$.
– Automorphismes de $\mathbb{Z}/n\mathbb{Z}$.
– Théorème de Sylow.

IV Exercices

104 - Groupes finis. Exemples et applications

Références [Per96], [AB], [Com98].

I Propriétés des groupes finis

• I.A Théorèmes fondamentaux

Soit G un groupe de cardinal fini.

Définition I.1 (Ordre)**.** Soit G un groupe fini. Son ordre est son cardinal. L'ordre $Ord(x)$ de x est l'ordre du sous-groupe $Gr(x)$. C'est aussi $\min\{n \in \mathbb{N}^* | x^n = 1\}$.

Exemple I.2.
- Si $k \in \mathbb{Z}/n\mathbb{Z}$, alors $Ord(k) = n/pgcd(n,k)$.
- Si $\sigma \in \mathfrak{S}_n$, alors $Ord(\sigma) = ppcm(\text{taille des cycles})$.

Proposition I.3. Si ϕ est un morphisme de groupes finis, alors $Ord(\phi(x))|Ord(x)$.

Applications I.4. Si G est un groupe abélien, alors : $Hom_{Gr}(\mathbb{Z}/n\mathbb{Z}, G) \cong G[n]$.

Théorème I.5 (Lagrange)**.**
- Si H est un sous-groupe de G, alors on a $\operatorname{Card} H | \operatorname{Card} G$.
- L'ordre d'un élément de G divise $\operatorname{Card} G$.

Applications I.6. Soient $q = p^k$ et n premier avec p, alors $\mathbb{F}_q$ contient une racine $n$em si et seulement si $n|q-1$.

Définition I.7. G est un p-groupes si son cardinal est une puissance de p.

Exemple I.8. $\mathbb{Z}/8\mathbb{Z}$, D_8 et $\mathbb{H}_8$ sont des 2-groupes.

• I.B Action d'un groupe fini sur un ensemble

Définition I.9. Une *action du groupe* G sur un ensemble X est un morphisme de groupe $G \to \mathfrak{S}(X)$. On note X^G l'ensemble des point fixes par le groupe G.

Exemple I.10.
- $\mathfrak{S}_n$ agit sur $K[X_1, \dots, X_n]$ par permutation des X_i.
- Soit $P(X) \in Q[X]$, alors son groupe de Galois agit ses racines.

Proposition I.11. Si G est un p-groupe alors $\operatorname{Card} X = \operatorname{Card} X^G \mod p$.

Théorème I.12 (Burnside)**.** On a $\operatorname{Card} Orbites. \operatorname{Card} G = \sum_{g \in G} \operatorname{Card} Fix(G)$.

Applications I.13. Développements Dénombrement des coliers de perles et dénombrement des coloriages du cube.

Applications

Proposition I.14 (Formule des classes)**.** Si Z est le centre de G arlos

$$\operatorname{Card} G = \operatorname{Card} Z + \sum_x \operatorname{Card} Cl(x),$$

où $Cl(x)$ est la classe de conjugaison de x et où x parcours une famille de représentants.

Applications I.15. Le centre d'un p-groupe est non trivial.

Théorème I.16 (Calay)**.** Tout sous-groupe fini est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Applications I.17. Tout groupe s'injecte dans un $GL_n(k)$ (et donc admet un p-Sylow cf plus bas).

Théorème I.18 (Cauchy)**.** Si p est une nombre premier divisant $\operatorname{Card} G$, alors il existe un élément d'ordre divisant G.

• I.C Sous-groupes de Sylow

Définition I.19. Un p-Sylow de G est un groupe d'ordre p^α avec $p^\alpha || \operatorname{Card} G$.

Exemple I.20.
- $\mathbb{Z}/3\mathbb{Z}$ est un 3-Sylow de $\mathbb{Z}/6\mathbb{Z}$.
- Les matrices triangulaires supérieures unipotents est p-Sylow de $GL_n(\mathbb{F}_p)$.

Théorème I.21 (Sylow)**.** Soit G un groupe fini, $\operatorname{Card} G = p^\alpha m$ avec $p \nmid m$. On note N le nombre de p-Sylow. Alors
- Tout sous-p-groupe est inclu dans un p-Sylow.
- Les p-sylow sont tous conjugués (donc $N | \operatorname{Card} G$).
- $N = 1 \mod p$ et $N|m$.

Applications I.22.
- Les groupes d'ordre < 60 ne sont pas simples ou sont trivialement simples.
- Développement Tout groupe simple d'ordre de 60 est isomorphe à $\mathfrak{A}_5$.

II Cas des groupes abéliens finis

• II.A Le groupe $\mathbb{Z}/n\mathbb{Z}$

Proposition II.1 (Générateurs)**.** Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les $d \mod n$ tels que $d \wedge n = 1$.

Définition II.2 (Indicatrice d'Euler)**.** On note $\phi(n)$ le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$.

Proposition II.3. Si $pgcd(n.m) = 1$, alors $\phi(nm) = \phi(n)\phi(m)$. Pour $n \in \mathbb{N}$, on a $\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$.

Applications II.4. Le $n$em polynôme cyclotomique est de degré

Proposition II.5 (Automorphismes)**.** On a $Aut(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}^\times$. Pour p premier impaire, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique. Pour $\alpha \geq 2$, on a $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

Proposition II.6 (Sous-groupes)**.** On a $\mathbb{Z}/N\mathbb{Z}[n] \simeq \mathbb{Z}/pgcd(n,d)\mathbb{Z}$.

Applications II.7. Pour p premier, on a $Hom_{Gr}(\mathbb{Z}/n\mathbb{Z}, Aut(\mathbb{Z}/p\mathbb{Z})) \simeq \mathbb{Z}/pgcd(p-1,n)\mathbb{Z}$

Applications II.8. Développement Classification des groupes d'ordre pq et des groupe d'ordre 12.

• II.B Structure des groupes abéliens finis

Définition II.9. Un groupe *monogène cyclique* est un groupe fini engendré par un élément.

Théorème II.10. Si G est un groupe monogène cyclique de cardinal n et si a est un générateur, alors l'application $\mathbb{Z}/n\mathbb{Z} \to G,\ n \mapsto a^n$ est un isomorphisme de groupe.

Proposition II.11. Si K est un corps commutatif et si G est un sous-groupe fini de K^*, alors G est cyclique.

Applications II.12. Le groupe des racines $n$em d'un corps est cyclique.

Proposition II.13. Soient G est un groupe non nécéssairement fini et Z son centre. Si G/Z est monogène, alors G est abélien.

Applications II.14. Les groupes d'ordre p^2 sont abéliens.

Théorème II.15 (Kronecker (ou diviseurs élémentaires))**.** Développement Soit G un groupe fini abélien. Alors il existe une unique famille $d_1|d_2|\cdots|d_p$ tel que G soit isomorphe à :$\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$.

Exemple II.16. $(\mathbb{Z}/12/\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

III Structure de quelques groupes finis

• III.A Le groupe $\mathfrak{S}_n$

Proposition III.1. Tout groupe fini G s'injecte dans $\mathfrak{S}(G)$.

Définition III.2 (Signature)**.** La signature d'une permutation est le nombre d'inversions.

Proposition III.3 (Générateurs)**.** Le groupe $\mathfrak{S}_n$ est engendré par les familles suivantes

- Les transpositions $(1,i)$.
- Les transpositions $(i,i+1)$.
- $(1,2)$ et $(1,\ldots,n)$.

Corollaire III.4. La signature est le seul automorphisme surjective de $\mathfrak{S}_n$ vers $\mathbb{Z}/2\mathbb{Z}$.

Applications III.5. Frobenius-Zolotarev : pour p premier impaire et $M \in \mathcal{M}_n(\mathbb{F}_p)$, on a $\varepsilon(M) = \left(\frac{\det M}{p}\right)$.

Théorème III.6. Développements [Simplicité] Le groupe $\mathfrak{A}_n$ est simple sauf pour $n = 4$.

Applications III.7. Il existe des polynômes non-résolubles par radicaux de degré aussi grand qu'on veut.

Théorème III.8. Développements [Automorphismes] Tous les automorphismes de $\mathfrak{S}_n$ sont intérieurs sauf pour $n = 6$.

Exemple III.9. L'action de $\mathfrak{S}_5$ sur ses 5-Sylow fournit un automorphisme non-intérieur.

• III.B Sous-groupes finis de $GL_n(\mathbb{R})$

Théorème III.10. Les sous-groupes finis de $O_2(\mathbb{R})$ sont isomorphe à $\mathbb{Z}/n\mathbb{Z}$ ou D_{2n}.

Théorème III.11. Développement Les sous-groupes finis de $SO_3(\mathbb{R})$ sont isomorphes à : $\mathbb{Z}/n\mathbb{Z}$, D_{2n}, $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$.

Théorème III.12 (Burnside)**.** Développement Si G est un sous-groupe d'exposant fini de $GL_n(\mathbb{R})$, alors G est cyclique.

IV Représentation des groupes finis

• IV.A Définitions

[A completer]

• IV.B Caractères

[A completer]

V Transformée de Fourier sur les groupes finis

• V.A Définition

[A completer]

• V.B Cas des groupes abéliens

[A completer]

VI Développements

- Sous-groupes finis de $SO_3(\mathbb{R})$.
- $\mathfrak{A}_5$ est le seul sous-groupe simple d'ordre 60.
- Théorème de Burnside.
- Théorème de Brauer
- Théorème de Sylow
- Sous-groupes d'ordre pq.
- Inversibles de $\mathbb{Z}/n\mathbb{Z}$.
- Simplicité de $\mathfrak{A}_n$
- Automorphisme de $\mathfrak{S}_n$.

VII Exercices

Exercice .1. Soit G un groupe fini et p le plus petit nombre premier divisant $Card(G)$. Montrer que si H est un sous-groupe d'indice p, alors H est distingué.

Démonstration. Le groupe G agit sur G/H, et on note K le noyau de cette action. On a alors $K = \bigcap_{x\in G} xHx^{-1} \subset H$. Le gorupe G/K s'injecte dans $\mathfrak{S}(G/H)$ de cardinal $p!$. Comme si q est un nombre premier divisnat l'indice de K, alors $q \geq p$ et q divise $p!$, doonc $q = p$ et $G = H$. Donc H est distingué. □

Exercice .2. Soit G un p-groupe. Montrer que pour tout $q|\operatorname{Card} G$, il existe un sous-groupe d'ordre q.

Démonstration. .[A completer] □

105 - Groupes des permutations d'un ensemble fini. Applications

Références [Tau], [Per96], [Com98], [AB].

I Groupe symétrique

• I.A Structure de $\mathfrak{S}_n$

Définition I.1. Pour $n \in \mathbb{N}$, le *groupe symétrique* $\mathfrak{S}_n$ est l'ensemble des bijections de $[1, n]$.

Proposition I.2. Le groupe $\mathfrak{S}_n$ est d'ordre $n!$.

Définition I.3. Soit $\sigma \in \mathfrak{S}_n$. L'orbite de $k \in [1, n]$ par σ est $O_\sigma(k) = \{\sigma^p(k) \mid p \in \mathbb{N}\}$. Son *support* est l'ensemble des points de $[1, n]$ non fixes par σ. Un *cycle* est une permutation ayant une seule orbite non réduite à un point.

Exemple I.4. $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix}$ est un 3-cylcle.

Proposition I.5. Si deux permutations sont à supports disjoints alors elle commutent. Toute permutation est de manière unique produit de cycles à supports disjoints et les supports de ces cycles sont les orbites.

Définition I.6. Une transposition est un cycle dont l'orbite non trivial est de cardinal 2.

Proposition I.7. Si $\gamma = (a_1, \dots, a_p)$ est un cycle alors. $\gamma = (a_1, a_2)...(a_{p-1}, a_p)$.

Proposition I.8 (Générateurs)**.**
- Les transpositions engendrent $\mathfrak{S}_n$.
- Les transpositions $(i, i+1)$ engendrent $\mathfrak{S}_n$
- la transposition $(1, 2)$ et le cycle $(1, 2, ..., n)$ engendrent $\mathfrak{S}_n$.

Applications I.9. Á conjugaison près, il y a que 3 morphisme de $\mathfrak{S}_4$ dans $\mathfrak{S}_3$.

Proposition I.10. Deux permutations sont conjugués si et seulement si les longueurs des cycles apparaissant dans leurs décompositions sont les mêmes.

• I.B Signature et groupe alterné

Définition I.11.
- La *signature* est $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j} \in \{-1, 1\}$. C'est le nombre d'inversions de la permutation.
- Une permutation est *paire* si sa signature est $+1$ et *impaire* sinon. Le *groupe alterné* $\mathfrak{A}_n$ est le sous-groupe des permutations pairs.

Proposition I.12. La signature est un morphisme de groupe surjectif de $\mathfrak{S}_n$ vers $\{-1, 1\}$ et c'est le seul.

Applications I.13.
- Frobenius-Zolotarev : pour p premier impaire et $M \in \mathcal{M}_n(\mathbb{F}_p)$, on a $\varepsilon(M) = \left(\frac{\det M}{p}\right)$.
- Développement Loi de réciprocité quadratique.

II Propriétés algébriques de $\mathfrak{S}_n$

Théorème II.1. Développements [Simplicité] Le groupe $\mathfrak{A}_n$ est simple sauf pour $n = 4$.

Corollaire II.2. Pour $n \geq 5$, le seul sous-groupe distingué on trivial de $\mathfrak{S}_n$ est $\mathfrak{A}_n$.

Proposition II.3. Développement Tout groupe simple d'ordre de 60 est isomorphe à $\mathfrak{A}_5$.

Proposition II.4 (Groupe dérivé)**.** Pour $n \geq 1$, le groupe dérivé de $\mathfrak{S}_N$ est $\mathfrak{A}_n$.

Théorème II.5. Développements [Automorphismes]
- Tous les automorphismes de $\mathfrak{S}_n$ sont intérieurs sauf pour $n = 6$.
- Pour $n = 6$, On a $Aut(\mathfrak{S}_6)/Int(\mathfrak{S}_6) \simeq \mathbb{Z}/2\mathbb{Z}$.

Exemple II.6. L'action de $PGL_2(\mathbb{F}_5)$ sur $P^1(\mathbb{F}_5)$ fournit un automorphisme non-intérieur de $\mathfrak{S}_6$.

III Actions du groupe symétrique

• III.A Application aux matrices

Déterminant Soit k un corps commutatif et $n \in \mathbb{N}^*$.

Théorème III.1. L'espace des formes n-linéaires alternée sur $\mathbb{R}^n$ est de dimension 1, engendré par $\det(X^1, \dots, X^n) = \sum_\sigma \prod_i x_i^{\sigma(i)}$.

Proposition III.2. Si $\sigma \in \mathfrak{S}_n$, et $X_1, \dots, X_n \in \mathbb{R}^n$, alors $\det(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = \varepsilon(\sigma) \det(X^1, \dots, X^n)$.

Applications III.3. Calcul du détermiant par pivot de Gauss.

Matrices de permutations Si $\sigma \in \mathfrak{S}_n$, alors la matrice $P_\sigma = [\delta_{i,\sigma(j)}]_{i,j}$ est dans $O_n(\mathbb{R})$.

Théorème III.4. Développement [Brauer] Si P_σ sont conjugué sous $GL_n(k)$ alors ils sont conjugué sous $\mathfrak{S}_n$.

Définition III.5. Une matrice *bistochastique* est une matrice à coefficients positifs et dont la somme de chaque et de chaque colonne vaut 1.

Théorème III.6. Développement [Birkhoff] L'ensemble des matrices bistochastique est un covexe compact dont les points extrémaux sont les matrices de permutations.

Sous-groupes fini de $SO_3(\mathbb{R})$

Théorème III.7.
- Le groupe des isométries du tétraèdre est isomorphe à $\mathfrak{A}_4$.
- Le groupe des isométries du cube est isomorphe à $\mathfrak{S}_4$.
- Développement Le groupe des isométries du dodécaèdre est isomorphe à $\mathfrak{A}_5$.

Théorème III.8. Développement Les sous-groupes finis de $SO_3(\mathbb{R})$: sont isomorphes à : $\mathbb{Z}/n\mathbb{Z}/$, D_{2n}, $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$. De plus si deux sous-groupes sont isomorphes, alors ils sont conjugués.

• III.B Action sur $K[X_1, \dots, X_n]$

Le groupe $\mathfrak{S}_n$ agit sur $K[X_1, \dots, X_n]$ par permutation des racines.

Définition III.9.
- Un polynôme P est dit *symétrique* si $\sigma.P = P$ ($\sigma \in \mathfrak{S}_n$) et antisymétrique si $\sigma.P = \varepsilon(\sigma)P$ ($\sigma \in \mathfrak{S}_n$).
- Pour $k \in [1, n]$, le $k$em polynôme symétrique élémentaire est le polynôme $S_k = \sum_{i_1<1_2<\dots<i_k} X_{i_1} \dots X_{i_k}$.

Proposition III.10. Développement L'application suivante est un isomorphisme

$$\begin{array}{ccc} K[T_1, \dots, T_n] & \longrightarrow & K[X_1, \dots, X_n] \\ P & \longmapsto & P(S_1, \dots, S_n) \end{array}.$$

Exemple III.11.
- $Van(X_1, \dots, X_n) = \prod_{i<j}(X_i - X_j)$ est antsymétrique.
- Les sommes de Newton sont symétriques. Exemple : $X^2+Y^2+Z^2 = S_1^2 - 2S_2$.

Applications III.12.
- Si F est une fonction polynômiale de $K[X_{i,j}|i, j]$ sur $\mathcal{M}_n(\mathbb{C})$ stable sur les classes de similitude, alors F est polynômiale en les coefficients de $\chi_{M(X_{i,j})}(T)$, où $M(X_{i,j})$ est la matrice $[X_{i,j}]_{i,j}$.
- ? ? ?

IV Extensions galoisiennes

Soit $P(X) \in \mathbb{Q}[X]$ et $X = \{x_1, \dots, x_n\}$ l'ensemble ses racines dans $\mathbb{C}$. On note L son coprs de décomposition

Proposition IV.1. Développement Pour p premier, il existe $P(X) \in \mathbb{Q}[X]$ de degré p tel que son groupe de Galois soit isomorphe à $\mathfrak{S}_p$.

Applications IV.2. Il existe des polynômes non-résolubles par radicaux de degré aussi grand qu'on veut.

Proposition IV.3. Soit $P(X) \in Q[X]$.
- Alors son groupe de Galois agit de façon transitive sur ses racines si et seulement si $P(X)$ est irréductibles.
- Et il agit par permutation paire si et seulement son discriminant est un carré dans $\mathbb{Q}$.

V Développements

- Loi de récipocité quadratique.
- Groupe des isométries des polyèdres.
- Pour p permier il existe une extension galoisienne de groupe de Galois $\mathfrak{S}_p$
- Groupes simple d'ordre 60.
- Simplicité de $\mathfrak{A}_n$.
- Automorphismes de $\mathfrak{S}_n$.
- Théorème de Brauer.
- Théorème de Birkhoff.
- Action de $\mathfrak{S}_n$ sur $K[X_1, \dots, X_n]$.

VI Exercices

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

Références [Per96], [Gob96], [MT86].

I Structure du groupe linéaire

Soit k un corps commutatif et E un espace vectoriel de dimension n. Le groupe linéaire $GL(E)$ est le groupe des inversibles des endomorphismes de E. Si $E = k^n$ on le note $GL_n(k)$.

• I.A Déterminant et groupe spécial linéaire

Définition I.1. Si $M \in M_n(k)$, on note $\det M = \sum_\sigma \varepsilon(\sigma) \prod_i m_{i,\sigma(i)}$.

Proposition I.2.
- Pour $M \in M_n(k)$, $M \in GL_n(k) \iff \det M \in k^*$.
- $\det : GL_n(k) \to k^*$ est un morphisme de groupe.

Définition I.3. La *comatrice* de M est la matrice des cofacteurs de M.

Proposition I.4.
- On a ${}^tCom(M)M = \det M.Id$.
- Si M est inversible, alors $M^{-1} = (\det M)^{-1}{}^tCom(M)$.

Applications I.5. Formules de Cramer : si A est inversible et si $AX = Y$, alors $x_i = \frac{\det(A_1,\dots,A_{i-1},Y,\dots,A_n)}{\det A}$, où les A_i sont les colonnes de A.

Définition I.6. Le *groupe spécial linéaire* est $SL_n(k) = \ker \det = \{A \in GL_n(k) : \det A = 1\}$.

Proposition I.7. $GL_n(k) = SL_n(k) \rtimes k^*$.

• I.B Générateurs et centre

Définition I.8. Les *matrice de transvertions* sont les matrices de la forme $E_{i,j}(\lambda)$. Une *matrice de dilatation* est une matrice de la forme $diag(1,\dots,\lambda,\dots,1)$. Une *transvection* (resp. *dilatation*) est une matrice conjuguée à une matrice de transvection (resp. dilatation).

Proposition I.9. Les transvection engendrent $SL_n(k)$. Les dilations et les transvections engendre $GL_n(k)$. Les dilatations engendrent $GL_n(k)$.

Applications I.10. Methode de Gauss : il existe P produit de transvections et telle que $PA \in T_n^+(k)$.

Proposition I.11. Si $n \geq 3$, les transvection sont conjugués.

Corollaire I.12 (Groupe dérivé).
- On a $D(GL(E)) = SL(E)$, sauf si ($n = 2$ et $k = \mathbb{F}_2$).
- On a $D(SL(E)) = SL(E)$, sauf si ($n = 2$ et $k = \mathbb{F}_2$) ou ($n = 2$ et $\mathbb{F}_3$).

Remarque I.13. On a $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$, et $D(SL_2(\mathbb{F}_3)) = \mathbb{H}_8$.

Proposition I.14 (Centre). Le centre de $GL(E)$ est k^*. Le centre de $SL(E)$ est $\mu_n(k)$.

• I.C Cas des corps finis

Proposition I.15 (Cardinalité).
- $\sharp GL_n(\mathbb{F}_q) = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.
- $\sharp SL_n(\mathbb{F}_q) = (q^n-1)(q^n-q)\cdots(q^n-q^{n-2})q^{n-1}$.

Applications I.16. Tout groupe fini admet un p-Sylow.

Théorème I.17 (Frobénius-Zolotarev). Si $p \geq 3$, $\varepsilon(M) = \det M^{(p-1)/2}$.

Applications I.18. Loi de réciprocité quadratique : pour p et q deux nombre premiers distincts, on a $(p^{(q-1)/2} \mod q).(q^{(p-1)/2} \mod q) = (-1)^{(p-1)(q-1)/2}$.

II Groupe linéaires sur $\mathbb{R}$ et $\mathbb{C}$

• II.A Propriétés topologiques

Proposition II.1. $GL_n(\mathbb{R})$ est un ouvert dense de $\mathcal{M}_n(\mathbb{R})$ et a deux composantes connexes ($GL_n(\mathbb{C})$ a uen composante connexe).

Applications II.2. Si $A, B, C, D \in M_n(\mathbb{R})$ commutent alors $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - BC)$.

Proposition II.3.
- Soit $A \in \mathcal{M}_n(\mathbb{C})$ tel que $\rho(A) < 1$. Alors $A \in GL_n(\mathbb{C})$ et $A^{-1} = \sum_{p=0}^{\infty} A^p$.
- Le produit et l'inversion sont des applications C^∞

Applications II.4. Théorème d'inversion local : si $f : \mathbb{R}^n \xrightarrow{C^k} \mathbb{R}^n$ est telle $D_0 f \in GL_n(\mathbb{R})$, alors f est un C^k-difféomorphisme au voisinage de 0.

Théorème II.5. Lie-Kolchin Si G est un sous-groupe connexe résoluble de $GL_n(R)$, alors il est trigonalisable.

• II.B Groupe orthogonal

Définition II.6. Le *groupe ortogonal* est $O_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) | {}^M M = I_n\}$. Le *groupe spécial orthogonal* est $SO_n(\mathbb{R}) = O_n(\mathbb{R}) \cap SL_n(\mathbb{R})$.

Proposition II.7 (Structure des isométries)**.** Tout éléments de $O_n(\mathbb{R})$ est conjugué à $diag(1, \dots, -1, \dots, R_{\theta_1})$, avec $R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$.

Corollaire II.8. Pour $n \geq 1$, le gorupe $SO_n(\mathbb{R})$ est connexe.

Applications II.9.
- Toute isométrie affine admet une décomposition canonique.
- Les rotations de $SO_3(\mathbb{R})$ sont déterminées par un vecteur unitaire et un angle.

Proposition II.10. $SO_2(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ en tant que groupe topologique.

Applications II.11. Définition de l'angle en géométrie.

Proposition II.12. $O_n(\mathbb{R})$ est engendré par les réflexions. Pour $n \geq 3$, $SO_n(\mathbb{R})$ est engendré par les retournements.

Corollaire II.13. Le groupe $SO_3(\mathbb{R})$ est simple.

Proposition II.14 (Décomposition polaire)**.** $S_n^{++}(\mathbb{R}) \times O_n(\mathbb{R}) \to GL_n(\mathbb{R})$ est un C^∞-difféomorphisme.

Corollaire II.15.
- $O_n(\mathbb{R})$ est un sous-groupe compact maximal.
- Deux matrices réelles unitairement semblables sont orthogonalement semblables.

Applications II.16. Développement [Enveloppe convexe du groupe orthogonal] On munit $\mathcal{M}_n(\mathbb{R})$ de la norme 2 subordonnée. Alors $B(\bar{0}, 1)$ est l'enveloppe convexe de $O_n(\mathbb{R})$ et $O_n(\mathbb{R})$ est l'ensembl des points extrémaux de $B(\bar{0}, 1)$.

Théorème II.17. Développement [Sous-groupes compacts de $GL_n(\mathbb{R})$] Tout sous-groupe compact de $GL_n(\mathbb{R})$ est conjugué à un sous-groupe de $O_n(\mathbb{R})$.

Théorème II.18. Développement Les sous-groupes finis de $SO_3(\mathbb{R})$ sont isomorphes à : $\mathbb{Z}/n\mathbb{Z}$, D_{2n}, $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$.

• II.C Sous groupes fermés de $GL_n(\mathbb{R})$

Définition II.19. Si G est un sous-groupe fermé de $GL_n(\mathbb{R})$, alors on définit son algèbre de Lie par $L_G = \{X \in \mathcal{M}_n(\mathbb{R}) : \forall t \in \mathbb{R}, exp(tX) \in G\}$.

Proposition II.20. L'algèdbre de Lie de G est un sous-espace vectoriel stable par crochet de commutation.

Théorème II.21. Développement [Cartan Von-Neumann] Tout-sous groupe fermé de $GL_n(\mathbb{R})$ est une sous-variété lisse et son espace tangent en I_n est son algèbre de Lie.

Exemple II.22.
- $L_{GL_n(\mathbb{R})} = \mathcal{M}_n(\mathbb{R})$, $L_{SL_n(\mathbb{R})} = \ker Tr$.
- $L_{O_n(\mathbb{R})} = L_{SO_n(\mathbb{R})} = Antsym_n(\mathbb{R})$.
- $SP(2n))(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) : {}^t MJM = J\}$, $L_{SP_{2n}(\mathbb{R})} = \{X \in \mathcal{M}_n(\mathbb{R}) : {}^X J + JX = 0\}$.

III Représentations linéaires de groupes finis

• III.A Représentation et sous-représentation irréductible

Définition III.1. Soit Γ un groupe fini. Une *représentation linéaire* est une morphisme de groupe $\Gamma \to GL_n(\mathbb{C})$. Le représentation est dite *irréductible* s'il n'y a pas de sous-espace stable strict. Un *morphisme* entre deux représentations est une application linéaire tel que : $\forall g \in \Gamma, f.g = g.f$.

Exemple III.2.
- $\mathfrak{S}_n \; rightarrow GL_n(\mathbb{C}),\ \sigma \mapsto P_\sigma$.
- Représentation régulière : $\Gamma \to GL_\Gamma(\mathbb{C}),\ g \mapsto [\delta_{h,g.k}]_{h,k}$.

Théorème III.3 (Schur)**.** Toute représntation est somme directe de représentations irréductibles.

Théorème III.4. Développement [Burnside] Un sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini est fini.

• III.B Fonction centrales et caractères

Définition III.5.
- Une fonction centrale sur Γ est une fonction $f : \Gamma \to \mathbb{C}$ constante sur les classes.
- Si V est une représentation, alors son *caractère* est $\chi_V : g \mapsto Tr(g)$.
- On munit l'espace des caractères du produit hermitien : $\langle f, h\rangle = \frac{1}{\text{Card}\,\Gamma} \sum_{g\in\Gamma} \bar{f}(g)h(g)$.

Théorème III.6.
- L'ensemble des caractères de représentations irrédutibles forment une base orthonromée des fonctions centrales.
- Il y a autant de représentations irréductibles que de classes de conjugaison dans Γ.
- Si $W_1, \dots, W_k$ sont les représentations irréductibles et V une représentation, alors $V = \bigoplus_{i=1}^k W_i^{\langle \chi_V, \chi_{W_i}\rangle}$.

IV Développements

- Sous-groupe compact de $GL_n(\mathbb{R})$. [Alessandri : Theme de geo]
- Théorème de Lie-Kolchin [Chambert-Loir : Algebre corporiel]

– Théorème de Brauer [Beck, Malick, Peyre : Obj. Agreg.]
– Théorème de Frobenius-Zolotarev. [Beck, Malick, Peyre : Obj. Agreg.]
– Théorème de Burnside (un sous-groupe de GL_n est d'exposant fini si et seulement si il est fini).
– Theorem de Cartan [Gonnord et Tosel].
– Decomposition polaire [Gonnord et Tosel].
– Décomposition d'Iwasawa.
– Décomposition de Bruhat.

V Exercices

Exercice .1 (Agreg 2010)**.** Montrer que pour $n \neq m$, les groupes $GL_n(\mathbb{R})$ et $GL_m(\mathbb{R})$ ne sont pas isomorphes.

Démonstration. Dénombrer les classes de conjugaisons du sous-goupe $GL_n(\mathbb{R})[2]$ des éléments d'ordre 2. □

107 - Sous-groupes finis de $O_2(\mathbb{R})$ et de $SO_3(\mathbb{R})$. Applications

Références [...]

I Structure du groupe orthogonal de $\mathbb{R}^2$ et $\mathbb{R}^3$

• I.A Espaces euclidiens et endomorphismes orthogonaux

On considère l'espace $\mathbb{R}^n$ $(n = 2, 3)$ muni de sa structure euclidienne orienté.

Définition I.1. Le *groupe orthognal* $O_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R})^t MM = I_n\}$ est le sous-groupe de $GL_n(\mathbb{R})$ conservant le produit scalaire. Le groupe spécial orthogonal est $SO_n(\mathbb{R}) = O_n(\mathbb{R}) \cap SL_n(\mathbb{R})$.

Exemple I.2. Pour F un sous-espace vectoriel, la symétries par rapport à F parallèlement à $F^\perp$ est un endomorphisme orthogonal.

Proposition I.3. $O_n(\mathbb{R})$ et $SO_n(\mathbb{R})$ sont des sous-groupes compacts.

Proposition I.4. Tout sous-groupe fini de $GL_n(\mathbb{R})$ (resp. $SL_n(\mathbb{R})$) de $\mathbb{R}$ est conjugué à un sous-groupe fini de $O_n(\mathbb{R})$ (resp. $SO_n(\mathbb{R})$).

• I.B Rotations, symétries et angles dans $\mathbb{R}^2$

Proposition I.5. Les matrices de $SO_2(\mathbb{R})$ sont de la forme $R_t = \begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix}$.

L'application $\begin{array}{ccc} \mathbb{U} & \longrightarrow & SO_2(\mathbb{R}) \\ e^{it} & \longmapsto & R_t \end{array}$ est un isomorphisme de groupe topologique.

Corollaire I.6.
- Le groupe $SO_2(\mathbb{R})$ est commutatif et connexe.
- Pour $t \in \mathbb{R}$, on a $R_t^{-1} = R_{-t}$.

Définition I.7. On appelle R_t la *rotation d'angle t*.

Proposition I.8. Les matrices de $O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$ sont du type $S_t = \begin{bmatrix} \cos t & \sin t \\ \sin t & -\cos t \end{bmatrix}$. C'est la symétrie orthogonal par rapport à la droite $\mathbb{R}(\cos \frac{t}{2}, \sin \frac{t}{2})$.

Corollaire I.9. Tous les éléments de $O_2(\mathbb{R})$ sont d'ordre 2.

Proposition I.10. Pour u, v deux vecteurs unitaires, il existe un unique $t \in \mathbb{U}$ tel que $R_t.u = v$ (c'est-à-dire que $SO_2(\mathbb{R})$ agit simplement transitivement sur S^1).

Définition I.11. On appelle $t = (u, v)$ l'*angle orienté* entre.

• I.C Rotations de $\mathbb{R}^3$

Proposition I.12. Si $R \in \mathbb{R}^3$, alors il existe une base orthonormée (e_1, e_2, e_3) telle que la matrice de R soit de la forme : $\begin{bmatrix} 1 & \\ & R_t \end{bmatrix}$. De plus si $R \neq Id$, alors $vect(e_1)$ est le sous-espace propre de R_t pour la valeur propre 1 et t est unique au signe près.

Définition I.13.
- La droite $vect(e_1)$ est l'*axe* de la rotation et t est son angle.
- Si u est un vecteur unitaire et $t \in \mathbb{R}$, alors la rotation d'axe u et d'angle t est la rotation R telle que si (u, v, w) est une base orthornomé, alors la matrice de R dans cette base est $\begin{bmatrix} 1 & \\ & R_t \end{bmatrix}$.

Proposition I.14 (Expression intrinsèque de la rotation)**.** Si R est la rotation d'axe u et d'angle t, alors on a

$$\forall x \; in\mathbb{R}^3, Rx = \langle u, x\rangle u + \cos t(x - \langle u, x\rangle u) + \sin tx \wedge u.$$

Définition I.15. Un *retournement* estune rotation d'angle π.

Proposition I.16. Les retournements engendre $SO_3(\mathbb{R})$.

Applications I.17. Le groupe $SO_3(\mathbb{R})$ est simple.

II Classification des sous-groupes finis

• II.A Sous-groupes finis de O_2

Définition II.1. Un polygône est *régulier* si tous ses cotés sont égaux et si tous ses angles sont égaux.

Proposition II.2. Les sous-groupes finis de $SO_2(\mathbb{R})$ sont les $\mathbb{Z}/n\mathbb{Z}$. Les sous-groupes finis de $O_2(\mathbb{R})$ sont les $\mathbb{Z}/n\mathbb{Z}$ et les D_{2n}.

Proposition II.3. Si P est un polygône régulier à n côtés, alors son groupe des isométries est isomorphe à D_{2n}, et les axes de symétries des réflexions préservant P passent par un sommet ou le centre d'un côté de P.

Applications II.4. Dénombrement de colliers de perles.

• II.B Sous-groupes finis de $SO_3(\mathbb{R})$

Définition II.5. Un polyèdre est *régulier* si toutes ses faces des polygônes isométriques, et l'ensemble des somemts adjacent à tout sommet s forment un polygône régulier.

Théorème II.6. Il existe 5 polyèdres réguliers.
- Le groupe des isométries du tétraèdre est isomorphe à $\mathfrak{A}_4$.
- Le groupe des isométries du cube/octaèdre est isomorphe à $\mathfrak{S}_4$.

– Développement Le groupe des isométries du dodécaèdre/icosaèdre est isomorphe à $\mathfrak{A}_5$.

Applications II.7. Dénombrement des coloriages du cube.

• II.C Sous-groupes finis de $O_2(\mathbb{R})$ et $SO_3(\mathbb{R})$

Théorème II.8. Développement Les sous-groupes finis de $SO_3(\mathbb{R})$ sont isomorphes à : $\mathbb{Z}/n\mathbb{Z}$, D_{2n}, $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$.

III Applications géométrie euclidienne affine

• III.A Sous-groupes fini du groupe des isométries affine

[A completer]

• III.B Groupes des pavages

Définition III.1. Pavage [A completer]

Théorème III.2. Il existe 5 groupe de pavage. [A completer]

IV Développements

– Isométrie de l'icosaèdre.
– Pavages du plan.
– Sous-groupes finis de $SO_3(\mathbb{R})$.
– Quaternions.

108 - Exemples de parties génétrices d'un groupe

Références [Per96], [Gob96], [Gou94], [Ave92]

I Généralités

• I.A Définitions et propriétés

Définition I.1. Soit G un groupe et $A \subset G$. Le *sous-groupe engendré* par A est le plus petit sous-groupe contenant G, on le note $Gr(A)$. Une partie A est *génératrice* si le groupe qu'elle engendre est G.

Proposition I.2. – On a $Gr(A) = \left\{ \prod_{i=1}^{n} a_i^{u_i} \mid a_i \in A, u_i \in \mathbb{Z} \right\}$.
- Si deux morphismes de groupes coïncident sur une partie génératrices alors elles coïncident partout.
- Si l'image d'un morphisme f contient une partie génératrice, alors f est surjective.

Exemple I.3. $\{6, 4\}$ engendre $2\mathbb{Z}$ dans $\mathbb{Z}$. $\{3 \mod 4\}$ engendre $\mathbb{Z}/4\mathbb{Z}$.

Définition I.4. Un groupe est *monogène* s'il est engendré par un élément. Un groupe est dit *cyclique* s'il est monogène et fini.

Exemple I.5. – Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n.
- Le groupe $\mathbb{R}/\mathbb{Z}$ n'est pas cyclique.

Théorème I.6. Soit G un groupe de cardinal N. Alors G admet une partie génératrice de cardinal au plus $\log_2 N$.

Définition I.7. Un groupe de *type fini* est un groupe engendré par une partie finie.

Théorème I.8 (Schwartz)**.** Si $p|Card(G)$, alors il existe un élément d'ordre p.

Corollaire I.9. Si $p|Card(G)$, G admet un sous-groupe d'ordre.

Corollaire I.10. Le groupe $\mathbb{Z}/p\mathbb{Z}$ est à isomorphisme près le seul groupe d'ordre p.

• I.B Groupes dérivés

Définition I.11. Le *groupe dérivé* est le groupe engendré par les commutateurs $[a, b] = aba^{-1}b^{-1}$. On le note $D(G)$.

Exemple I.12. – Un groupe G est abélien si et seulement si $D(G) = \{1\}$.
- $D(S_n) = A_n$ pour $n \geq 5$.

II Groupes abéliens

• II.A Classification des groupes abéliens de type fini

Proposition II.1. Si G est engendré par n éléments, alors G est un quotient de $\mathbb{Z}^n$.

Théorème II.2 (Diviseurs élémentaires)**.** Soit G un groupe abélien de type fini, alors il existe une unique famille de nombres $r \in \mathbb{N}$, $d_1|d_1|...|d_p$ telle que $G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_p\mathbb{Z}$

Exemple II.3. – $(\mathbb{Z}/12\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

• II.B Groupes monogènes

Théorème II.4. Un groupe monogène est isomorphe à $\mathbb{Z}$ s'il est de cardinal infini et à $\mathbb{Z}/n\mathbb{Z}$ s'il est de cardinal fini n.

Théorème II.5. k engendre $\mathbb{Z}/n\mathbb{Z} \iff pgcd(k, n) = 1 \iff k \mod n \in \mathbb{Z}/n\mathbb{Z}^*$.

Exemple II.6. L'ensemble des racines n^{em} de l'unité $\mathbb{U}_n$ dans $\mathbb{C}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et $e^{2ik\pi/n}$ engendre $\mathbb{U}$ si et seulement si $pgcd(k, n) = 1$.

Applications II.7. Arithmétique : on note ϕ l'indicatrice d'Euler. Alors $\mathbb{Z}/n\mathbb{Z}$ admet $\phi(n)$ générateurs. Le $n$em polynôme cyclotomique est de dregré $\phi(n)$.

Théorème II.8. – Le groupe $\mathbb{F}_q^*$ est cyclique, donc isomorphe à $\mathbb{Z}/q - 1\mathbb{Z}$.
- Tout sous-groupe fini de k^* avec k un corps commutatif est cyclique. En particulier l'ensemble des racine $n$em de l'unité est cyclique.

Théorème II.9. Le groupe $\mathbb{Z}/n\mathbb{Z}^*$ est cyclique si et seulement si $n = 2, 4, p^l, 2p^l$.

III Groupes non-abéliens

• III.A Exemple du groupe symétrique

Définition III.1. $\mathfrak{S}_n$ est le groupe des bijections de $[1, n]$. Le groupe $\mathfrak{A}_n$ le groupe des permuations paires.

Théorème III.2. Le groupe $\mathfrak{S}_n$ est engendré par
- Les cycles.
- Les transpositions $(1, i)$.
- Les transpositions $(i, i + 1)$.
- $(1, 2)$ et $(1, ..., n)$.

Théorème III.3. Le groupe A_n est engendré par les 3-cycles.

Applications III.4. – Étude de $Hom(S_n, S_m)$. A conjugaison près il y a morphisme de groupe de $S_4 \to S_3 : 1, \epsilon$, projection $S_4 \to V \rtimes S_3$.

- Les morphismes de $S_n \to k^*$ sont 1 et ε.
- Développement A_n est simple pour $n \geq 5$
- Développement Pour p premier, il existe $P(X) \in \mathbb{Q}[X]$ de degré p tel que son groupe de Galois soit isomorphe à $\mathfrak{S}_p$.

• III.B Groupes Libres

Définition III.5. Le *groupe libre* de rang n est :$F_n = \{$ mots de n lettres munie de la concaténation $\}$

Théorème III.6. Si G est un groupe et $g_1, \ldots, g_n \in G$ alors il existe un unique morphisme de groupe $\phi : F_n \to G$ tel que $\phi(a_i) = g_i$.

Théorème III.7. Tout groupe de type fini engendré par n élément est un quotient de F_n.

Définition III.8. On appelle *relations* de F_n un sous-groupe distingué de F_n. On dit qu'un groupe est de *présentation finie* s'il est isomorphe à F_n/R avec $n \in \mathbb{N}$ et R un sous-groupe distingué finiment engendré.

Exemple III.9. Groupe diédral : $D_{2n} = Gr(r,s) = F_2/(r^n = 1, s^2 = 1, srs^{-1} = r^{-1})$.

Applications III.10 (Banach-Tarski faible)**.** Il existe :
- D une partie dénombrable au plus de $\mathbb{S}^2$.
- Une partition de $\mathbb{S} \setminus D$ en 4 partie : $\mathbb{S} \setminus D = A_1 \sqcup A_2 \sqcup A_3 \sqcup A_4$
- Deux rotations $f, g \in SO_3(\mathbb{R})$. Tels que
$$S \setminus D = A_1 \sqcup a(A_2) = A_3 \sqcup b(A_4).$$
(On admettra que $\mathbb{Q} \cap \cos(\mathbb{Q}\pi) = \{\pm 1., \pm 1/2, 0\}$).

IV Groupe linéaire et sous-groupes

• IV.A Groupe linéaire et spécial linéaire

Définition IV.1. Une *transvection* de $\mathbb{R}^n$ est un endomorphisme du type $Id + u.\phi$ avec $\phi(u) = 0$ et $u \neq 0$, $\phi \neq 0$. Une *dilatation* est un endomorphisme de la forme $Id + u.\phi$ avec $\phi(u) \neq 0, -1$ et $u \neq 0$, $\phi \neq 0$. Une *matrice de transvection* est une matrice de la forme $\begin{pmatrix} 1 & \lambda \\ & 1 \end{pmatrix}$.

Théorème IV.2. Soit k un corps
- Le groupe $GL_n(k)$ est engendré par les matrices de transvections et de dilations.
- Le groupe $GL_n(k)$ est engendrée par les dilatations.
- Le groupe $SL_n(k)$ est engendré par les transvections.

Applications IV.3.
- Le groupe $SL_n(\mathbb{R})$ est connexe.
- Si $A \in GL_n(\mathbb{R})$, alors la mesure image de A est $(\det A)^{-1} d\lambda$.

• IV.B Groupe orthogonal et spécial orthogonal

• IV.C Groupe orthogonal

Définition IV.4. Le *groupe ortogonal* est $O_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) |^M M = I_n\}$. Le *groupe spécial orthogonal* est $SO_n(\mathbb{R}) = O_n(\mathbb{R}) \cap SL_n(\mathbb{R})$.

Proposition IV.5 (Structure des isométries)**.** Tout éléments de $O_n(\mathbb{R})$ est conjugué à $diag(1, \ldots, -1, \ldots, R_{\theta_1})$, avec $R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$.

Corollaire IV.6. Pour $n \geq 1$, le gorupe $SO_n(\mathbb{R})$ est connexe.

Applications IV.7.
- Toute isométrie affine admet une décomposition canonique.
- Les rotations de $SO_3(\mathbb{R})$ sont déterminées par un vecteur unitaire et un angle.

Proposition IV.8. $SO_2(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ en tant que groupe topologique.

Applications IV.9. Définition de l'angle en géométrie.

Proposition IV.10. $O_n(\mathbb{R})$ est engendré par les réflexions. Pour $n \geq 3$, $SO_n(\mathbb{R})$ est engendré par les retournements.

Corollaire IV.11. Le groupe $SO_3(\mathbb{R})$ est simple.

• IV.D Groupe modulaires

Le groupe modulaire $SL_2(\mathbb{Z})$ agit sur $\mathcal{H} = \{\text{Im} > 0\}$ par homographie.

Théorème IV.12. Développement Le groupe $SL_2(\mathbb{Z})$ est engendré par les mtrices $T\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

V Développements

- Théorème de Banach-Tarski.
- Action du groupe modulaire.
- $\mathfrak{S}_p$ est groupe de Galois.
- Groupes des isométries des polyèdres.
- A_n est simple pour $n \geq 5$.
- Théorème de Frobenius-Zolotarev.
- Transformée de Fourier sur les groupes finis.

VI Exercices

109 - Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications

Références [Com98], [AB], [Per96], [Dem97].

I Structure de $\mathbb{Z}/n\mathbb{Z}$

• I.A Congruence modulo n

Définition I.1 (Espace $\mathbb{Z}/n\mathbb{Z}$)**.** Soient $n \in \mathbb{N}^*$ et $a, b \in Z$. On dit que a est congru à $b \mod n$ si $n|b-a$. Celà définit une relation d'équivalence et on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes.

Proposition I.2. Munie des lois $\bar{a}+\bar{b} = a \bar{+} b$ et $\bar{a}.\bar{b} = \bar{ab}$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un anneau unitaire commutatif.

Proposition I.3. Pour $n \in \mathbb{N}^*$ et $a \in a\mathbb{N}$, on a
- $Caract(\mathbb{Z}/n\mathbb{Z}) = n$
- $\mathbb{Z}/n\mathbb{Z}$ intègre $\iff Z/n\mathbb{Z}$ est un corps $\iff n$ est premier.
- $a \in \mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $pgcd(a,n) = 1$.

Proposition I.4. Tout corps de caractéristique fini $p > 0$ contient le corps $\mathbb{Z}/p\mathbb{Z}$.

Définition I.5 (Indicatrice d'Euler)**.** L'indicatrice d'Euler de n est $\phi(n) = \text{Card}((\mathbb{Z}/n\mathbb{Z})^\times)$.

Proposition I.6. Soit $n \in \mathbb{N}^*$ et $x \in \mathbb{Z}^*$.
- Si $p = n^\alpha$, alors $\phi(p^\alpha) = p^{\alpha-1}(p-1)$.
- Fermat : $x^{\phi(n)} = 1 \mod n$.
- Wilson : p est premier si et seulement si $(p-1)! = -1 \mod [p]$.

Théorème I.7 (Lemme Chinois)**.** Si n et m sont premiers entre eux alors l'application $\begin{array}{ccc} \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ x \mod nm & \longmapsto & (x \mod n, x \mod m) \end{array}$ est un isomorphisme d'anneau.

Applications I.8. Résolution de systèmes de congruence.

Proposition I.9.
- Le groupe $\mathbb{U}_n$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
- Le sous-groupe de torsion $\mathbb{Z}/n\mathbb{Z}[m]$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$ avec $d = pgcd(n,m)$.

Applications I.10.
- Le corps $\mathbb{F}_q$ contient une racine primitive $n$eme de l'unité si et seulement si $n|q-1$.
- On a $Hom(\mathbb{Z}/n\mathbb{Z}/, \mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/pgcd(n,m)\mathbb{Z}$.

• I.B Automorphismes de $\mathbb{Z}/n\mathbb{Z}$

Proposition I.11. $Aut_{Gr}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}^\times$.

Théorème I.12. Développement Pour p premier impaire, le groupe $\mathbb{Z}/p^\alpha\mathbb{Z}$ est cyclique : $\mathbb{Z}/p^\alpha\mathbb{Z}^\times \cong \mathbb{Z}/p^\phi\mathbb{Z} = \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$. Et pour $p = 2$:
- $\mathbb{Z}/2\mathbb{Z}^\times = \{1\}$.
- Pour $\alpha \geq 2$, $\mathbb{Z}/2^\alpha\mathbb{Z}^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

• I.C Lien avec le groupe des racines de l'unité

Théorème I.13. L'application $\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{U}_n \\ k & \longmapsto & e^{2ik\pi/n} \end{array}$ est un isomorphisme de groupe.

Définition I.14. Polynômes cyclotomiques : $\Phi_n(X) = \prod_{pgcd(k,n)=1}(X - e^{2ik\pi/n})$.

Applications I.15. Développement Théorème de dirichlet : pour $n \geq 2$, il existe une infinité de nombre premier congrus à $1 \mod n$.

II Applications l'étude des groupes

Proposition II.1. Tout groupe d'ordre p avec p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Applications II.2. Tout groupe d'ordre p^2 est abélien.

Théorème II.3 (Structure des groupe abéliens de type fini)**.** Si G est un groupe abélien de type fini, alors G est isomorphe à un produit unique produit de $\mathbb{Z}^r$ par $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$ avec $d_1|\cdots|d_s$. On appelle r le rang de G et $d_1, \ldots, d_s$ ses diviseurs élémentaires.

Exemple II.4. $(\mathbb{Z}/15\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Proposition II.5. Les seuls groupes d'ordre 4 sont $\mathbb{Z}/4\mathbb{Z}$ et $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Théorème II.6. Développement
- Les groupes d'ordre pq, avec p, q premiers tels que $q > p$, sont $\mathbb{Z}/pq\mathbb{Z}$ ou $\mathbb{Z}/qZ \rtimes Z/p\mathbb{Z}$ si $p|q-1$.
- Les groupes d'ordre 12 sont : $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \rtimes V_4$, $V_2 \rtimes \mathbb{Z}/3\mathbb{Z}$ (on utilsera le théorème de Sylow).

III Polynômes sur $\mathbb{Z}/n\mathbb{Z}[X]$

Théorème III.1 (Critère d'irréductibilité)**.** Pour $P \in \mathbb{Z}[X]$ unitaire, si $P(X)$ est irréductible dans un $\mathbb{F}_p[X]$, alors $P(X)$ est irréductible dans $\mathbb{Z}[X]$.

Exemple III.2. ???

Exemple III.3. $X^4 + 1$ est réductible dans tous les $\mathbb{Z}/p\mathbb{Z}$.

Théorème III.4 (Critère d'Eisenstein)**.** Soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. S'il existe p premier tel que $P(X) = X^n \mod p$ et $p^2 \nmid a_0$, alors $P(X)$ est irréductible sur $\mathbb{Z}[X]$.

Applications III.5. $\Phi_{p^\alpha}(X)$ et $X^n - 2$ sont irréductibles.

IV Cas du corps $\mathbb{F}_p$

V Généralités

Définition V.1. Symbole de Legendre : $\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p \in \{-1, 1\}$.

Proposition V.2. Pour $a \in \mathbb{F}_p^\times$, a est un carré si et seulement si $\left(\frac{a}{p}\right) = 1$.

Applications V.3. Développements Entiers de Gauss et théorème des deux carrés.

Théorème V.4. Développement [Loi de réciprocité quadratique] Pour p, q premier on a $\left(\frac{q}{p}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.

Théorème V.5 (Frobenius-Zolotarev)**.** Pour p premier impaire et $M \in \mathcal{M}_n(\mathbb{F}_p)$, on a $\varepsilon(M) = \left(\frac{\det M}{p}\right)$.

VI Codes correcteurs

[A completer]

• VI.A Applications arithmétiques

RSA [A completer]

Tests de primalités de Fermat [A completer]

Définition VI.1. Nombres de Carmichael. [A completer]

Théorème VI.2 (Korselt)**.** Développement [A completer]

VII Développements

- Loi de réciprocité quadratique.
- Groupes d'ordre 12.
- Entiers de Gauss et théorème des deux carrées.
- Inversibles de $\mathbb{Z}/n\mathbb{Z}$.
- Théorème de Dirichlet.
- Théorème de Fermat pour $n = 4$.
- Théorème de Dirichlet :
- Théorème de Frobénius-Zolotarev.

VIII Exercices

Exercice .1 (Goudon Chap 1.1 Ex 4)**.** (Nombres de Mersennes) Soit $a \geq 2$ et $n \geq 2$. Si $a^n - 1$ est premier montrer que $a = 2$ et que n est premier.

Démonstration. Si $n = pq$ est une décomposition de n avec $p \leq q$, Alors $a^n - 1 = (a^p - 1)(1 + a^p + \cdots + a^{p(q-1)})$. Comme $a^n - 1$ est premier, soit $a^p - 1 = 1$ auquel cas $a = 2$ et $p = 1$, soit $(1 + a^p + \cdots + a^{p(q-1)}) = 1$ auquel cas $q = 1$, puis $n = 1$, ce qui contredit l'hypothèse $n \geq 2$. □

Remarque VIII.1. $2^{11} - 1 = 23.49$ n'est pas premier.

Exercice .2 (Goudon Chap 1.1 Ex 4)**.** (Nombres de Fermat) Soit $n \in \mathbb{N}$. Montrer que si $2^n + 1$ est premier, alors n est une puissance de 2.

Démonstration. Si $n = 2^s t$ est la décomposition de n en puissance de 2 fois un nombre impaire, alors $2^n + 1 = (2^{2^t} + 1)(1 - 2^{2^t} + \cdots + (-1)^{s-1} 2^{2^t s})$. Comme $2^n + 1$ est premier celà implique $(1 - 2^{2^t} + \cdots + (-1)^{s-1} 2^{2^t s}) = 1$, soit $s = 1$. □

Remarque VIII.2. $2^{2^5} + 1 = 641.6700417$ (Euler). On ne connait d'autres nombres de Fermat premier au delà.

Exercice .3 (Gourdon Chap 1.1 Ex 7)**.** (Dirichlet cas $-1 \mod 6$) Montrer qu'il y a une infinité de nombres premier du type $6k - 1$.

Démonstration. S'il existe qu'un nombre fini de nombre premiers $p_1, \ldots, p_s$ congrues à $-1 \mod 6$. On note $N = -1 + 6p_1 \ldots p_s$. On a alors $N = -1 \mod 6$. Si q est un facteur premier de N, alors $q = \pm 1 \mod 6$, et q n'est pas l'un des p_i. Donc $q = 1 \mod 6$ et tous les facteurs premiers de N sont congrues à $1 \mod 6$, ce qui contredit $N = -1 \mod 6$. □

110 - Nombres premiers. Applications

Références [Combes ?]

I Propriétés des nombres premiers

• I.A Arithmétiques sur les entiers

Définition I.1. – Un entier naturel $p \in \mathbb{N}^*$ est un nombre premier si ses seuls diviseurs sont 1 et p (i.e. p est irréductible dans le langage des anneaux).
– Un entier non premier est dit composé.

On note P l'ensemble des nombres premiers.

Proposition I.2. L'ensemble des nombres permiers est infini.

Proposition I.3. Si p est premier et si $p|bc$, alors $p|a$ ou $p|b$ (i.e. p est premier dans le langage des anneaux).

Théorème I.4 (Factorisation)**.** – Crible d'Erasthotène : tout entier n admet un diviseur premier $\leq \sqrt{n}$.
– Tout entier n se décompose de façon unique en $\prod_{p\in P} p^{v_p(n)}$. On appelle $v_p(n)$ la valuation p-adique de n.

Proposition I.5. Si n est non premier, alors n admet un diviseur premier inférieur à $\sqrt{n}$.

Applications I.6. – Développement [Théorème des deux carrés] Tout nombre.
– Développement [Théorème des quatre carrés].

Définition I.7. – Nombre de Mersenne : $M_n = 2^n - 1$.
– Nombre de Fermat : $F_n = 2^{2^n} + 1$.

Proposition I.8. Si M_n est premier, alors n est une puissance de 2.

Remarque I.9. Les 4 premiers nomrbes de Fermat sont premiers. Les 16 suivant sont composées. On en connais pas d'autre qui sont premiers.

Proposition I.10 (Polygônes constructibles)**.** ...

• I.B Répartition des nombres premiers

Proposition I.11. Pour tout $n \in \mathbb{N}$, il existe un intervalle d'amplitude n qui ne contient pas de nombres premiers.

Théorème I.12 (Équivalent)**.** On note $\pi(x)$ la nombre de nombre premier $\leq x$, alors $\pi(x) \sim x/\ln(x)$.

Théorème I.13 (Postulat de Bertrand)**.** .

Théorème I.14. Développement [Dirichlet]

Définition I.15. Fonction de Möbius.

Proposition I.16 (Formule Inversion)**.** ...

Théorème I.17. Développement [Probabilité que deux nombres soient premier entre eux] .

• I.C Corps $\mathbb{Z}/p\mathbb{Z}$

Proposition I.18. Pour $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est une corps si et seulement si n est premier.

Théorème I.19 (Fermat)**.** $x^{p-1} = 1 \mod p$.

Proposition I.20. Soit p premier. Pour $n \in \mathbb{F}_p^*$, on a : $n \in \mathbb{F}_p^* \iff n^{(p-1)/2} = 1$.

Définition I.21. Pour $n \in \mathbb{F}_p^*$, sont symbole de Legendre est $\left(\frac{n}{p}\right) = n^{(p-1)/2}$.

Théorème I.22 (Frobenius-Zolotarev)**.** $\varepsilon(M) = \left(\frac{\det M}{p}\right)$.

Théorème I.23 (Loi de réciprocité quadratique)**.** Soient p, q deux nombres premiers ≥ 3.
– $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.
– $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Applications I.24. – Tests de primalités des nombres de Fermat : si $F_k = 2^{2^k} + 1$ (avec $k \geq 1$), alors F_k est premier si et seulement si $3^{(F_k-1)/2} = -1 \mod F_k$.
– Cas particulier du théorème de Dirichlet : il existe une infinité de nombre premier congrue à $1 \mod 4$ (resp. $1 \mod 6$, resp. $-1 \mod 10$).

• I.D Critère de primalité

Proposition I.25 (Critère de Fermat)**.** Si n est premier, alors : $\forall a \in [1, n-1], a^n = a \mod n$.

Définition I.26. Un entier n est de *Carmikael* si : $\forall a \in [0, n-1], a^n = a \mod n$.

Théorème I.27 (Korselt)**.** Un nombre n est de Carmikael si et seulement si n est sans facteur carré et pour tout nombre premier p divisant n on a $p-1|n-1$.

Exemple I.28. Les trois premiers nombres de Carmikael sont : 561, 1105, 1729.

II Applications des nombres premiers

• II.A Théorie des groupes

Proposition II.1. Soit G un groupe.
- Si $p|\operatorname{Card} G$, alors il existe un élément d'ordre p.
- Pour tout p, G admet N p-Sylow avec $N = 1 \mod p$ et $N|\operatorname{Card} G$.
- ???

Proposition II.2. Si p est premier, et si τ est une transposition et γ un p-cycle de $\mathfrak{S}_p$ alors (τ, γ) engendrent $\mathfrak{S}_p$.

Théorème II.3. Développement Pour p premier, $\mathfrak{S}_p$ est un groupe de Galois.

• II.B Utilisation de la réduction modulo p

Théorème II.4 (Eisenstein)**.** Soit $P \in \mathbb{Z}[X]$ tel que $P \mod p = aX^n$, avec $a \neq 0 \mod p$ et $P \mod p^2 = aX^n + b$, avec $b \neq 0 \mod p^2$. Alors P est irréductible.

Théorème II.5. S'il existe, p tel que $P \mod p$ est irréductible, alors P est irréductible.

Proposition II.6. ???.

III Développements

- $\mathfrak{S}_p$ est un groupe de Galois.
- Loi de réciprocité quadratique.
- Probabilité pour que deux nombres soient premiers entre eux.
- Théorème de Dirichlet
- Théorème de Sylow.
- Théorème de Fermat pour $n = 4$.
- Groupes d'ordre pq.

IV Exercies

111 - Anneaux principaux. Applications

Références [Com98], [Tau].

I Généralités

• I.A Définitions et propriétés

Soit $\mathbb{A}$ un anneau unitaire commutatif intègre.

Définition I.1. Un *idéal* est sous-groupe absorbant pour la multiplication. On note (a) ou $a\mathbb{A}$ l'idéal engendrépar a.

Proposition I.2. Si I est un idéal strict de $\mathbb{A}$, alors $\mathbb{A}/I$ muni des lois $\bar{a}+\bar{b} = a \bar{+} b$ et $\bar{a}.\bar{b} = \bar{ab}$ est un anneau commutatif.

Définition I.3. Un idéal I est *principal* s'il est engendré par un élément. L'anneau $\mathbb{A}$ est *principal* si et seulement si $\mathbb{A}$ est intègre est tous ces idéaux sont principaux.

Proposition I.4.
- Tout anneau principal est noethérien.
- Tout idéal premier non nul est maximal.

• I.B Anneaux euclidiens

Définition I.5. Un *stathme euclidien* sur A est une application $N : A \setminus \{0\} \to \mathbb{N}$ vérifiant : $\forall a, b \in A, \exists q, r \in A, a = bq + r$ et $r = 0$ ou $N(r) < N(b)$. Un anneau est *eucldien* s'il admet un stathme euclidien.

Remarque I.6. Si un stathme existe, alors il existe un stathme qui vérifie en plus : $a|b \Rightarrow N(a) \geq N(b)$. Celà permet de prouver qu'un anneau euclidien est factoriel sans utiliser l'axiome du choix.

Proposition I.7. Tout anneau euclidien est principal.

Exemple I.8.
- $\mathbb{Z}$ est euclidien pour la norme.
- $K[X]$ est eucliden pourle degré

Remarque I.9. Développement $\mathbb{Z}[(1+\sqrt{-19})/2]$ est principal mais non factoriel

Tous les idéux de $\mathbb{Z}/6\mathbb{Z}$ sont principaux, mais tous les éléments ne sont pas décomposables en irréductibles.

II Arithmétique dans un anneau

• II.A Relations de divisibilité

Définition II.1. On se place dans un anneau $\mathbb{A}$ intègre. On dit que a *divise* b si : $\exists c \in A, ac = b$. On dit que a est *associé* à b si : $\exists c \in A^\times, ac = b$.

Proposition II.2.
- Si $(a) = (b)$, alors a et b sont associés.
- Si $a|b$ alors $(a) \supset (b)$.

Définition II.3. Un *pgcd* de a et b est un diviseur commun d de a et b et tel que tout diviseur commun divise d. Un *ppcm* est un multiple commun m à a et b et tel que tout multiple commun est un multiplde de m.

Théorème II.4 (Bezout)**.** Si $\mathbb{A}$ est principal, alors $d = pgcd(a, b)$, alors $(d) = (a) + (b)$ et il existe $u, v \in A$ tel que $d = au + vb$.

Corollaire II.5 (Lemme de Gauss)**.** Pour A principal, si $a|bc$ et $pgcd(a, b)$, alors $a|c$.

Définition II.6. Un élément a est *irréductible* si $a = pq \to p$ ou $q \in A^\times$. Un élément est dit premier si $a|bc \to a|b$ ou $a|c$. Un élément a est *premier* si : $\forall b, c \in \mathbb{A}, a|bc \Longrightarrow a|b$ ou ac.

Proposition II.7. Dans un anneau principal, tout élément irréductible est premier.

• II.B Anneaux factoriels

Définition II.8. L'anneau A est *factoriel* tout élément admet une unique décomposition en facteurs irréductibles.

Proposition II.9. Dans un anneau factoriel le *pgcd* existe et est donné par

$$pgcd(u\prod p^{\alpha_p}, v\prod p^{\beta_p}) = \prod p^{\min(\alpha_p,\beta_p)}.$$

Remarque II.10. Le lemme de Bezout est faux si l'anneau est seulement factoriel.

Théorème II.11. Soit $\mathbb{A}$ un anneau intègre. Alors : $\mathbb{A}$ principal $\Longrightarrow$ $\mathbb{A}$ noethérien et l'intersection deux idéaux principaux est encore principal $\Longrightarrow$ est factoriel.

Applications II.12. Développement $\mathbb{A}$ principal $\Longrightarrow$ $\mathbb{A}[[X]]$ factoriel.

Remarque II.13. Les ideaux de $\mathbb{Z}/6\mathbb{Z}$ sont principaux, mais tous les éléments ne sont pas décomposable en irrductibles.

III Modules sur un anneau principal

• III.A Généralités

Définition III.1. Soit $\mathbb{A}$ un anneau intègre. Un $\mathbb{A}$-module est un groupe abélien M muni d'une action $A \to Hom_{Gr}(M)$

Proposition III.2. Si M est un $\mathbb{A}$-module libre de rang n, alors tout sous-module est libre de rang $\leq n$.

Applications III.3. ???

• III.B Classification est A-modules de type fini

Théorème III.4. Soit M un $\mathbb{A}$-module de type fini. Alors il existe une unique famille $r \in \mathbb{N}$ et $d_1 | \cdots | d_n$ tel que $M \simeq \mathbb{A}^r \times \mathbb{A}/d_1\mathbb{A} \times \cdots \times \mathbb{A}/d_n\mathbb{A}$.

Applications III.5 (Classifitation des groupes abéliens de type fini)**.** Tout groupe abélien de type fini est isomorphe à $\mathbb{Z}^r \times \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$, alors $d_i | d_{i+1}$.

IV Arithmétique sur $\mathbb{Z}[i]$

Théorème IV.1. Développement L'anneau $\mathbb{Z}[i]$ est euclidien pour la norme.

Applications IV.2 (Théorème des deux carrés)**.** Un entier est somme de deux carrés si et seulement si chacun de ses facteurs premiers de la forme 4k + 3 intervient à une puissance paire.

Théorème IV.3. Développement Pour $d < 0$, l'anneau $\mathbb{Z}[\sqrt{d}]$ est euclidien pour la norme si et seulement si $d = -1, -2, -3, -7, -11$.

Théorème IV.4. Développement Théorème des quatre carrés avec les quaternions.

V $K[X]$

• V.A Applications en algèbre linéaire

Proposition V.1. Pour K corps $K[X]$ est euclidien pour le degré. (et $\mathbb{A}[X]$ est principal, alors $\mathbb{A}$ est un corps).

Théorème V.2 (Idéaux premier de K[X,Y)**.**]Développement .

• V.B Applications en algèbre linéaire

Définition V.3.
- Le *polynôme minimal* d'un endomorphisme u est le générateur unitaire μ_u de $\{P \in K[X] : P(u) = 0\}$ (de degré $\leq n$ par Calay-Hamilton).
- Un endomorphisme est cyclique si le degré de son polynôme minimal est n. Auquel cas il existe x tel que $(x, u(x), \ldots, u^{n-1}(x))$ soit une base de E, auquel cas la matrice de u est $Frob(\mu_u)$.

Théorème V.4 (Décomposition de Frobénius)**.** Si f est endomorphisme d'un k-espace vetoriel de dimension finie, alors il existe une base tel que la matrice de f soit $Diag(Frob(P_1(X)), \ldots, Frob(P_n(X)))$, avec $P_i | p_{i+1}$.

Applications V.5.
- Décomposition de Jordan.
- Le polynôme minimal est invriant par extension scalaire.
- Les classes de similitudes sont invariants par extension scalaire.

Définition V.6. Un endomorphisme est *semi-simple* si tout sous-espace stable admet un supplémentaire stable.

Théorème V.7. Développement [Endomorphisme semi-simple] $u \in L(E)$ est semi-simple si et seulement si μ_u est sans facteru carré.

VI Développements

- $\mathbb{A}[[X]]$ est factoriel.
- Entiers de Gauss et théorème des deux carrés.
- Endomorphisme semi-simple.
- $\mathbb{Z}[(1 + \sqrt{19})/2]$ est principal et non factoriel.
- Pour $d < 0$ sans facteur carré, $\mathbb{Z}[\sqrt{d}]$ est euclidien pour le stathme norme si et seulement si $d \in \{-1, -2, -3, -7, -11\}$
- Idéaux premiers de $K[X, Y]$.

Exercice .1. Soit E un A-module libre de rang fini. Soit F un sous-module. A quelle condition F admet un supplémentaire.

Démonstration. .[A compelter]. □

Exercice .2 (Gourdon Chap 1.1 Ex 2)**.** (Amélioration de Bezout) Soient $a, b \in \mathbb{Z}$ premiers entre eux. Montrer qu'il existe $u, v \in \mathbb{Z}$ tel que $|u| < |b|$ et $|v| < a$ tels que $au + bv = 1$.

Démonstration. Soient $u_0, v_0 \in \mathbb{Z}$ tels que $au + bv = 1$. Soit $v = aq + r$ la division euclidienne de a par u. Alors $a(u + bq) + br = 1$. Ce qui donne $\dfrac{u + bq}{b} = \dfrac{1}{ab} - \dfrac{r}{a} \in]-1, 1[$. □

l

112 - Corps finis. Applications

Références [Per96], [Lidl], [Escofier, Alg. licence].

I Construction des corps finis

• I.A Les corps premiers $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

On rappelle que pour $n \in \mathbb{N}^*$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ une structure d'anneau.

Proposition I.1. Pour $n \in \mathbb{N}^*$, on a : $\mathbb{Z}/n\mathbb{Z}$ est un corps $\iff$ $\mathbb{Z}/n\mathbb{Z}$ est un intègre $\iff$ n est premier.

Le corps $\mathbb{Z}/p\mathbb{Z}$ est un corps monogène de cardinal p et de caractéristique p. On le note $\mathbb{F}_p$.

Théorème I.2 (Fermat)**.** $x^{p-1} = 1 \mod p$.

• I.B Extensions de $\mathbb{Z}/p\mathbb{Z}$

Proposition I.3. Soit k un corps fini non nécessairement commutatif (a posteriori commutatif par théorème de Wedderburn), p sa caractéristique et q son cardinal. Alors :
- p est un nombre premier.
- Il y a une unique injection de $\mathbb{Z}/p\mathbb{Z}$ dans k.
- Il existe $n \in \mathbb{N}^*$ tel que $q = p^n$.

Proposition I.4. Si k est commutatif, la groupe multiplicatif k^* est cyclique.

Le *corps de décomposition* d'un polynôme $P(X) \in \mathbb{F}_p[X]$ est une extension de $\mathbb{F}_p$ où $P(X)$ est simplement scindé et minimale pour cette propriété. On se donne p un nombre premier et $q = p^n$ avec $n \in \mathbb{N}^*$.

Proposition I.5 (Corps de décomposition)**.** Le corps de décomposition de $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$, noté $D_p(X^q - X)$, est de cardinal q.

Théorème I.6 (Unicité des corps finis)**.** Si k est un corps commutatif à q éléments alors $K \simeq D_p(X^q - X)$.

Remarque I.7. On note $\mathbb{F}_q$ le corps commutatif q éléments. En fait $\mathbb{F}_q$ est un réprésentant d'une classe d'isomorphime de corps. Si p est premier, on peut dire que le corps $\mathbb{F}_p$ est unique, car si deux corps sont deux cardinal p, il n'y a qu'un seul isomorphisme de corps entre eux.

Théorème I.8 (Wedderburn)**.** Tout corps fini gauche est commutatif.

Proposition I.9. Soient $q = p^n$ et $q' = p^{n'}$. Alors $\mathbb{F}_{q'}$ contient un sous-corps isomorphe à $\mathbb{F}_q$ si et seulement si q' est une puissance de q, c'est-à-dire que n divise n'.

• I.C Clôture de $\mathbb{Z}/p\mathbb{Z}$

On pose $K_p = \varinjlim \mathbb{F}_{p^{n!}}$, l'où on s'est fixé une famille d'injections $\mathbb{F}_{p^{n!}} \to \mathbb{F}_{p^{n+1!}}$.

Théorème I.10. Le corps K_p est la clotûre algébrique de $\mathbb{F}_p$.

On notera $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$.

II Propriétés algébriques des corps finis

• II.A Racines de l'unité

Le groupe des racines de l'unité $U_n(k)$ d'un corps k est cyclique d'ordre divisant n. Dans $\overline{\mathbb{F}}_p^*$ tous les éléments sont des racines de l'unité. On remarque que si $n = q - 1$, alors $U_n(\overline{\mathbb{F}}_p) = \mathbb{F}_q^*$.

Proposition II.1. Dans $\overline{\mathbb{F}}_p$, si n s'écrit $p^\alpha n'$, avec $p \wedge n' = 1$, alors le groupe $U_n(\overline{\mathbb{F}}_p)$ est isomorphe à $\mathbb{Z}/n'\mathbb{Z}$.

Dans $\mathbb{F}_q$, on a aussi $U_n(\mathbb{F}_q) = U_{n'}(\mathbb{F}_q)$.

Proposition II.2. On suppose que $p \wedge n = 1$. Alors $U_n(\mathbb{F}_q)$ est de cardinal $pgcd(n, q-1)$.

En particulier $\mathbb{F}_q$ contient une racine primitive de l'unité si et seulement si n divise $q - 1$, ce qui est équivalent à r est multiple de l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^*$.

• II.B Groupe des automomorphismes

Définition II.3. Soit $q = p^n$ et $r = q^m$. le *Frobénius* $\begin{array}{rccc} Frob_q : & \mathbb{F}_r & \longrightarrow & \mathbb{F}_r \\ & x & \longmapsto & x^q \end{array}$ est un morphisme de $\mathbb{F}_q$-extensions.

Proposition II.4.
- Le Frobénius est un automorphisme de $\mathbb{F}_q$-algèbre.
- Le groupe de Galois $Gal(\mathbb{F}_r/F_q)$ est cyclque de cardinal m engendré par $Frob_m$.

• II.C Matrices sur les corps finis

Théorème II.5. Pour $A \in M_n(\mathbb{F}_q)$, A est diagonalisable si et seulement si $A^q = A$.

Théorème II.6 (Frobenius-Zolotarev)**.** $\varepsilon(M) = \left(\dfrac{\det M}{p}\right)$.

• II.D Carrés dans $\mathbb{F}_p$

Proposition II.7. Soit p premier. Pour $n \in \mathbb{F}_p^*$, on a : $n \in \mathbb{F}_p^* \iff n^{(p-1)/2} = 1$.

Définition II.8. Pour $n \in \mathbb{F}_p^*$, sont symbole de Legendre est $\left(\frac{n}{p}\right) = n^{(p-1)/2}$.

Théorème II.9 (Loi de réciprocité quadratique)**.** Soient p, q deux nombres premiers ≥ 3.

- $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.
- $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Applications II.10.

- Tests de primalités des nombres de Fermat : si $F_k = 2^{2^k} + 1$ (avec $k \geq 1$), alors F_k est premier si et seulement si $3^{(F_k-1)/2} = -1 \mod F_k$.
- Cas particulier du théorème de Dirichlet : il existe une infinité de nombre premier congrue à $1 \mod 4$ (resp. $1 \mod 6$, resp. $-1 \mod 10$).

Proposition II.11. Si $p \geq 3$, les formes quadratiques sur $\mathbb{F}_p$ sont du type $diag(1, \dots, 1, 0, \dots)$ ou $diag(1, \dots, 1, a, 0, \dots)$ avec $a \in \mathbb{F}^* \setminus \mathbb{F}_p^{*n} c2$.

III Polynômes sur $\mathbb{F}_q$

• III.A Polynômes irréductibles

Pour $n \in \mathbb{N}^*$, on note $I_n(\mathbb{F}_q)$, le nombre de polynômes irréductibles sur $\mathbb{F}_q$ de degré n.

Théorème III.1 (Décomposition en irréductibles)**.** La décomposition de $X^{q^n} - X$ en irréductibles est :$X^{q^n} - X = \prod_{d|n} \prod_{P \in I(K,d)} P$.

Théorème III.2 (Dénombrement)**.** On a

- Pour tout $n \in \mathbb{N}, q^n = \sum_{d|n} d|I(K,d)|$.
- Pour tout $n \in \mathbb{N}, I(K,n) \neq \emptyset$.
- Pour tout $n \in \mathbb{N}, I(K,n) = \frac{1}{n} \sum_{d|n} \mu_{n/d} q^d$.
- On a $|I(1,K)| = q$.
- Si $Caract(K) \neq 2, |I(2,K)| = \frac{q(q-1)}{2}$

Exemple III.3. $X^2 + X + 1$ es le seul irréductible de $\mathbb{F}_2[X]$ de degré 2, et $\mathbb{F}_2[X]/(X^2 + X + 1) \simeq \mathbb{F}_4$.

Théorème III.4. Développement [Berlekamp] [A completer].

• III.B Critère d'irréductiblité sur $\mathbb{Z}[[X]]$

Théorème III.5. Si $P(X) \in \mathbb{Z}[X]$ untaire est irrédutible dans $\mathbb{F}_p[X]$, pour un certain p, alors P est irrédutible dans $\mathbb{Z}[X]$.

Théorème III.6 (Critère d'Eisenstein)**.** Soit $P(X) = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$. On suppose que

- p ne divise pas a_n.
- p divise a_i pour $i \in [0, n-1]$.
- p^2 ne divise pas a_0.

Alors $P(X)$ est irréductible dans $\mathbb{Z}[X]$.

Exemple III.7. Le polynômes $\Phi_p(X)$ et $X^n - 2$ sont irréductibles sur $\mathbb{Z}[X]$.

• III.C Polynômes cyclotomiques

On définit les polynômes cyclotomiques $\Phi_n(X) = \prod_{d \wedge n = 1} X - e^{2ik\pi/n} \in \mathbb{C}[X]$ et on rappelle que ce sont des polynômes dans $\mathbb{Z}[X]$ et qu'on a la décomposition en irréductibles $X^n - 1 = \prod_{d|n} \Phi_d(X)$ dans $\mathbb{Z}[X]$.

Dans $\overline{\mathbb{F}}_p$, si n s'écrit $n = p^\alpha n'$, alors $X^n - 1 = (X^{n'} - 1)^{p^\alpha}$.

Proposition III.8 (Racines des polynômes cyclotomiques)**.**

- Si p ne divise pas n (on a alors $U_n(\overline{\mathbb{F}}_p) \simeq \mathbb{Z}/n\mathbb{Z}$), alors $\Phi_n(X) = \prod_{d \wedge n = 1} X - \zeta_n^d$, où ζ_n est une racine primitive $n$em de l'unité dans $\overline{\mathbb{F}}_p$.
- Si $n = p^\alpha n'$, alors $\Phi_n(X) = \Phi_n(X)^{\phi(p^\alpha)} = \Phi_n(X)^{p^\alpha - p^{\alpha-1}}$.

Sur $\mathbb{F}_q$ les polynômes $\Phi_d(X)$ ne sont pas irréductibles.

Proposition III.9 (Décomposition en irréductibles)**.** On suppose que p ne divise pas n et $q = p^r$. Alors dans $\mathbb{F}_q[X]$, $\Phi_n(X)$ est produit de (r ?) facteurs de degré s où s est l'ordre que q dans $\mathbb{Z}/n\mathbb{Z}^\times$.

IV Codes correcteurs linéaires

V Généralités

[A compléter]

VI Codes cycliques

[A compléter]

VII Développements

- Loi de réciprocité quadratique.
- Théorème de Chevalley-Warning.
- Théorème de Wedderburn.
- Théorème de Frobenius-Zolotarev.
- Dénombrement des irréductibles.

VIII Exercices

113 - Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications

Références [AB].

I Structure de $\mathbb{U}$

• I.A Définitions et propriétés

Définition I.1. On note $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$. Géométriquement $\mathbb{U}$ est le cercle unité de $\mathbb{C}$. C'est une sous-variété lisse connexe compact de $\mathbb{C}$.

Proposition I.2. $\mathbb{U}$ est un groupe topologique isomorphe à $\mathbb{R}/\mathbb{Z}$ via l'application $t \mod \mathbb{Z} \mapsto e^{2i\pi t}$. Géométriquement $2\pi t$ représente l'angle entre $e^{2\pi t}$ et 1.

Proposition I.3 (Décomposition polaire)**.** L'application $\begin{array}{ccc} \mathbb{R}_+^* \times \mathbb{U} & \longrightarrow & \mathbb{C}^* \\ (r,u) & \longmapsto & ru \end{array}$ est une bijection (aussi un C^∞-difféormorphisme)

Définition I.4. On appelle *argument* d'un nombre complexe z non nulle, l'angle de $z/|z|$.

Proposition I.5. Pour $z, w \in \mathbb{C}^*$, on a $Arg(zw) = Arg(z) + Arg(w)$.

Proposition I.6 (Relèvement de l'angle)**.** Si $\mathbb{R} \to \mathbb{U}$ est une application C^1, alors il existe une application $\theta : \mathbb{R} \to \mathbb{R}$ C^1 telle que $g = exp(i\theta)$.

Applications I.7. Si $f : \Omega \to \mathbb{C}^*$ est une fonction holomorphe, alors il existe $h : \Omega \to \mathbb{C}$ tel que $f = exp(g)$.

• I.B Sous-groupes de $\mathbb{U}$

Définition I.8. Une racine $n$em de l'unité est une nombre complexe $z \in \mathbb{C}$, tel que $z^n = 1$.

Proposition I.9.
- L'ensembles des racines $n$eme de l'unité est le groupe $\{e^{2ik\pi/n} | k \in [0, n-1]\} \simeq \mathbb{Z}/n\mathbb{Z}$ et c'est le seul sous-groupe d'ordre n de $\mathbb{U}$.
- Si G est un sous-groupe de $\mathbb{U}$ infini, alors G est dense dans $\mathbb{U}$.

Exemple I.10.
- Le sous-groupe engendré par $e^{2i\pi t}$ est dense si et seulement si θ est non rationnel.
- L'ensemble des points rationnels de $\mathbb{U}$ est un sous-groupe dense de $\mathbb{U}$.
- L'ensemble des points de torsions de $\mathbb{U}$ est un sous-groupe dense.

Applications I.11.
- $\begin{array}{ccc} \mathbb{U} & \longrightarrow & \mathbb{T}^2 \\ t & \longmapsto & (e^{it}, e^{i\pi t}) \end{array}$ est une droite dense dans le tore.
- Les caractères continues de $\mathbb{U}$ sont du type $t \mapsto e^{ikt}$.

II Applications à la géométrie

• II.A Notion d'angle dans $\mathbb{R}^2$

Définition II.1. On note $SO_2(\mathbb{R})$ le groupe des rotations positives de $\mathbb{R}^2$.

Proposition II.2. En identifiant $\mathbb{R}^2$ à $\mathbb{C}$, l'action de $\mathbb{U}$ sur $\mathbb{C}$ fournit un isomorphisme entre $\mathbb{U}$ et $SO_2(\mathbb{R})$.

Définition II.3. $SO_2(\mathbb{R})$ agit simplement transitivement sur $\mathbb{U}$. L'angle entre deux vecteurs (u, v) est l'élément t tel que $R_t.u = v$.

Définition II.4. On note $j = e^{2\pi/3}$.

Proposition II.5. Soient $a, b, c \in \mathbb{C}$. Alors abc forment un triangle équilatéral direct si et seulement si $a + bj + cj^2 = 0$.

Applications II.6.
- Théorème de Napoléon : soit ABC un triangle, et PRQ les centres des triangles équilatéraux extérieurs à ABC. Alors PQR est un triangle équilatéral.
- Théorème de Morley : L'intersectection des trisectrices d'un triangle est un triangle équilatéral.

• II.B Représentation des isométries du plan

Proposition II.7 (Représentations des isométries)**.** Les isométries directes de $\mathbb{C}$ sont du type $e^{i\alpha}(z - w) + w$ et les isométries indirectes sont du type $e^{i\alpha}\overline{z - w} + w$.

Applications II.8. Développement [Droite de Simson] .

• II.C Action des quaternions sur $\mathbb{R}^3$

Soit E un espace euclidien orienté. Le corps des quaternions est $\mathbb{R} \oplus E$, muni la multiplication $(x + \vec{u}).(y + \vec{v}) = xy - \vec{u}.\vec{v} + x\vec{u} + y\vec{v} + \vec{u} \wedge \vec{v}$. On le note $\mathbb{H}$. On munie aussi $\mathbb{H}$ de la norme euclidienne et de la conjugaison $\overline{(x + u)} = x - u$. On note U l'ensemble des quaternions de norme 1. On appelle E l'espace des quaternions purs.

Proposition II.9 (Structure des quaternions)**.**
- $\mathbb{H}$ est un corps non commutatif dont le centre est $\mathbb{R}$.
- La norme est multiplicative.
- Tout quaternion non nul s'écrit de façon unique sous la forme rn avec $r \in \mathbb{R}_+$ et $n \in U$.
- La multiplication par $q \in U$ est un élément de $SO(\mathbb{H})$.

Proposition II.10. Developpement Alors on a un isomophisme $U/\{\pm 1\} \cong SO(E)$. Si $q = \cos\theta + \sin\theta u$ est un quaternion unitaire alors la conjugaison par q est la rotation d'angle 2θ autour de u.

III Polynômes cyclotomiques

• III.A Racines primitives de l'unité

Définition III.1. Une racine primitive de l'unité est un nombre complexe z tel que z engendre $\mathbb{U}_n$.

Proposition III.2. Les racines primitives de l'unité sont du type $e^{i2k\pi/n}$ avec $k \wedge n = 1$.

Le groupe $\mathbb{U}_n$ a exactement $\phi(n)$ générateurs.

Définition III.3. Le $n$em polynôme cyclotomique est $\Phi_n(X) = \prod_{k\wedge n=1} (X - e^{2i\pi k/n})$.

Proposition III.4. Les polynômes cyclotomiques sont à coefficients dans $\mathbb{Z}$.

Applications III.5. On peut définir les polynômes cyclotomique dans n'importe quel anneau, en particuleir on peut réduire modulo p.

• III.B Propriétés de $\Phi_n(X)$

Théorème III.6 (Irréductilité)**.** Développement Les polynôme cyclotomiques sont irréductibles dans $\mathbb{Z}[X]$. La décomposition de $X^n - 1$ en irréducible est $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Applications III.7 (Brauer)**.** Développement Si deux permutations sont conjugués dans $GL_n(\mathbb{C})$, alors il sont conjugués dans $\mathfrak{S}_n$.

Applications III.8 (Dirichlet)**.** Développement Pour $n \in \mathbb{N}_{\geq 2}$, il existe une infinité de nombre premier congrus à $1 \mod n$.

Théorème III.9 (Kronecker)**.** Développement Si $P(X)$ est un polynôme irréductible de $\mathbb{Z}[X]$ tel que toutes ses raciens sont de module inférieur à 1, alors $P(X) = X$ ou $P(X)$ est un polynôme cyclotomique.

IV Transformée de Fourier

• IV.A Caractère d'un groupe

Définition IV.1. Soit G un groupe topologique compact. Un caractère de G est un morphisme de groupe continue $G \to \mathbb{C}^*$. On note G^* l'ensemble des caractères de G.

Proposition IV.2. Les caractères sont à valeurs dans le cercle unité

Exemple IV.3. $\mathbb{Z}/N\mathbb{Z}^* = \mathbb{U}_n$.

Définition IV.4. Mesure de Haar sur G : mesure invariante à gauche et à droite et finie sur tout compact.

Proposition IV.5. La mesure de Haar existe.

• IV.B Transformée de Fourier sur $\mathbb{U}$

Proposition IV.6. Les caractères de $\mathbb{U}$ sont les $(e^{ikx})_{k\in\mathbb{Z}}$.

V Développements

- Irréductibilité des polynôme cyclotomique.
- Théorème de Brauer.
- Théorème de Dirichlet.
- Théorème de Kronecker.
- Droite de Simson.
- Quaternions.

114 - Anneaux des séries formelles. Applications

Références [Cal06], [Gob96], [Lan02] [Arnaudies 1].

I Structures de $A[[X]]$

• I.A Définitions

Soit A un anneau (intègre) commutatif.

Définition I.1. Pour $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$, leur *produit de convolution* $(c_n)_{n\in\mathbb{N}} = (a_n) * (b_n)$ est défini par $c_n = \sum_{p+q=n} a_p b_q$.

Définition I.2. L'anneau des *séries formelles* $A[[X]]$ sur A est $A^{\mathbb{N}}$ muni du produit de convolution. L'élément $(a_n) \in K^{\mathbb{N}}$ sera noté $\sum_{n=0}^{+\infty} a_n X^n$.

L'anneau $A[[X]]$ est une A-algèbre commutative unitaire d'élément neutre $1 = (1, 0, \dots)$ et contient naturellement $A[X]$.

Exemple I.3. $\sum_{n=0}^{+\infty} X^n$, $Exp(X) = \sum_{n=0}^{+\infty} \frac{X^n}{n!}$, $Ln(1+X) = \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n} X^n$.

• I.B Propriétés algébriques et topologiques

Définition I.4. Pour $F \in A[[X]]$, la *valuation* de $F(X)$ est

$$val(F) = inf\{n \in \mathbb{N} \mid a_n \neq 0\} \text{ (valant } +\infty \text{ si } F(X) = 0).$$

Proposition I.5. La valuation vérifie les propriétés suivantes
- $val(F) = +\infty \Leftrightarrow F = 0$.
- $val(F+G) \geq \min(val(F), val(G))$ avec égalité si $val(F) \neq val(G)$.
- $val(FG) = val(F) + val(G)$.

Corollaire I.6. L'application

$$\begin{array}{rccc} d: & K[[X]] \times K[[X]] & \longrightarrow & K[[X]] \\ & (F, G) & \longmapsto & e^{-val(F-G)} \end{array}$$

définit une distance ultramétrique ($|F(X) + G(X)| \leq \max(|F(X)|, |G(X)|)$) sur $K[[X]]$.

Une suite $(F_n(X))_{n\in\mathbb{N}}$ tend alors vers 0 si et seulement si $(val(F_n(X)))_{n\in\mathbb{N}}$ tend vers $+\infty$.

Théorème I.7 (Complétude)**.** Muni de cette distance, $K[[X]]$ est un anneau topologique (c'est-à-dire que les lois d'anneau sont continues) complet. De plus $K[[X]]$ est la complétion de $K[X]$.

Comme la distance est ultramétrique, une série converge si et seulement si son terme général tend vers 0.

Proposition I.8 (Inversibles et idéaux)**.**
- $F(X)$ est inversible si et seulement si $a_0 \in A^\times$. Auquel cas son inverse est $F(X)^{-1} = a_0^{-1} \sum_{n=0}^{\infty} (1 - a_0^{-1} F(X))^n$.
- Si $A = K$ est un corps alors de plus $K[[X]]$ est principal et tous les idéaux stricts sont de la forme (X^n).

En particulier $K[[X]]$ est factoriel et X est l'unique élément irréductible.

Proposition I.9. Si A est noetherien, alors $A[[X]]$ est noetherien.

Théorème I.10. Développement Si A est principal, alors $A[[X]]$ est factoriel.

On utilisera les résultats suivants

Proposition I.11. Si B est un anneau noetherien et si $\forall a, b \in B, (a) \cap (b)$ est idéal principal, alors B est factoriel.

Lemme I.12 (Nakayama)**.** Soit M un B-module de type fini et $x \in B$. On suppose que $xM = M$, alors il existe $a \in B$ tel que $a = 1 \mod x$ et $aM = 0$.

• I.C Opérations sur les séries formelles

Composition des séries formelles

Définition I.13. Pour $F, G \in A[[X]]$ avec $F(X) = \sum_{n=0}^{\infty} a_n X^n$ et G de valuation non nulle, la série $\sum_{n=0}^{+\infty} a_n G(X)^n$ converge dans $A[[X]]$ et on note $F \circ G(X)$ sa somme. On dit que F est la *réciproque* de G si $val(F) > 0$ et $F \circ G = G \circ F = 0$.

Exemple I.14. Si $F = exp(X) - 1$ et $G = Ln(1+X)$, alors F est la réciproque de G.

Proposition I.15. On a $val(F \circ G) = val(F).val(G)$. L'application

$$\begin{array}{ccc} A[[X]] & \longrightarrow & A[[X]] \\ F & \longmapsto & F \circ G \end{array}$$

est un morphisme de A-algèbre continue.

Théorème I.16. Pour $G \in K[[X]]$ de valuation non nulle, G admet une réciproque si et seulement si $a_1(G) \in A^\times$

Dérivation

Définition I.17. Pour $F(X) = \sum_{n=0}^{+\infty} a_n X^n \in A[[X]]$, sa *série dérivée* est

$$F'(X) = \frac{dF}{dX}(X) = \sum_{n=0}^{+\infty} (n+1) a_{n+1} X^n.$$

Proposition I.18.
- Formule de Leibniz : la dérivation est continue et pour $F, G \in A[[X]]$, on a $(F.G)' = F'G + GF'$.
- Si $val(G) > 0$, alors $(F \circ G(X))' = F' \circ G(X).G'(X)$.
- Noyau de la dérivation : si A est de caractéristique 0, alors $F'(X) = 0$ si et seulement si $F(X)$ est constant. Si A est de caractéristique p, alors $F'(X) = 0$ si et seulement si $a_n = 0$ pour n non multiple de p

• I.D Corps des fractions

Soit K un corps. On note $K((X))$ les séries formelles de la forme $\sum_{n=v}^{+\infty} a_n X^n$. avec $v \in \mathbb{Z}$. Pour $F \in K((X))$, on note toutjours $val(F) = inf\{n \in \mathbb{Z} | a_n \neq 0\}$ et d la distance définie précédemment.

Théorème I.19. L'espace $K((X))$ est un corps topologique et $K((X)) = Frac(K[[X]])$.

Remarque I.20. On a pas $Frac(A[[X]]) = Frac(A)((X))$ en général .

II Suites et séries génératrices

• II.A Définitions

Définition II.1. Soit $(a_n)_{n\in\mathbb{N}}$ une suite. Sa *série génératrice* est $\sum_{n=0}^{+\infty} a_n X^n$.

Sa *série génératrice exponentielle* est $\sum_{n=0}^{+\infty} \frac{a_n}{n!} X^n$.

Exemple II.2. Si Y est une variable aléatoire sur $\mathbb{N}$, alors on peut regarder $F_Y(T) = \sum_{n=0}^{+\infty} P(Y = n) T^n$.

• II.B Règles de calcul

Proposition II.3. Si $F(X)$ est la série génératrice de $(a_n)_{n\in\mathbb{N}}$, $G(X)$ celle de $(b_n)_{n\in\mathbb{N}}$ alors
- $F(X).G(X)$ est la série génératrice de $(\sum_{p+q=n} a_p b_q)_{n\in\mathbb{N}}$.
- $(F(X) - a_0)/X$ est la série génératrice de $(a_{n+1})_{n\in\mathbb{N}}$.
- $XF'(X)$ est la série génératrice de $(na_n)_{n\in\mathbb{N}}$.

Applications II.4 (Calcul des moments)**.** Si Y est une variable aléatoire L^2, alors $E[Y] = F_Y'(1)$ et $Var(Y) = F_Y''(1) + F_Y'(1) - F_Y'^2(1)$.

Applications II.5. Développement Dénombrement des solutions de $\{\alpha_1 p_1 + \cdots + \alpha_k p_k = n\}$

Proposition II.6. Si $F(X)$ est la série génératrice exponentielle de $(a_n)_{n\in\mathbb{N}}$, $G(X)$ celle de $(b_n)_{n\in\mathbb{N}}$ alors
- $F(X).G(X)$ est la série génératrice de $\left(\sum_{p+q=n} \binom{n}{p} a_p b_q\right)_{n\in\mathbb{N}}$.
- $F'(X)$ est la série génératrice de $(a_{n+1})_{n\in\mathbb{N}}$.

Exemple II.7. Si D_n est le nombre de partitions de $[1, n]$, alors $D_{n+1} = \sum_{k=1}^{n} \binom{n}{k} D_{n-k}$. Si $F(T)$ est la série génératrice exponentielle de $(D_n)_{n\in\mathbb{N}}$, alors $F'(T) = exp(T).F(T)$.

III Fonctions définies par une série formelle

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

• III.A Séries entières

Définition III.1. Si $F(X) \in \mathbb{C}[[X]]$, le *rayon de convergence* de $F(X)$ est

$$R = sup\{r \geq 0 \mid \sum_{n\in\mathbb{N}} |a_n| r^n < +\infty\}$$

L'ensembles des séries de rayon de convergence non nul est une sous-algèbre de $\mathbb{C}[[X]]$.

Proposition III.2.
- Les séries $F(X)$ et $F'(X)$ ont même rayon de convergence.
- Si $F(X) \in \mathbb{C}[[X]]$ a un rayon $R > 0$, alors $F : z \mapsto \sum_{n\in\mathbb{N}} a_n z^n$ définit une fonction sur $D(0, R)$, et la fonction définie est dérivable de dérivé la fonction définie par $F'(X)$.

Applications III.3. On peut utiliser des outils d'analyse (par exemple les équations différentielles) pour résoudre des équations dans $\mathbb{C}[[X]]$.

Applications III.4. $1 + X$ admet pour racine carré $\sum_{n\in\mathbb{N}} \binom{n}{1/2} X^n$ dans $\mathbb{Q}[[X]]$.

• III.B Séries de matrices dans $M_n(\mathbb{R})$ ou $M_n(\mathbb{R})$

Proposition III.5. Si $F(T)$ a pour rayon de convergence R, alors pour $X \in M_n(\mathbb{C})$ de rayon spectral $< R$, la série $\sum_{n\in\mathbb{N}} a_n X^n$ converge. On note $F(X)$ sa somme.

En particulier $F(A)$ existe si A est nilpotent ou si $R = +\infty$.

Théorème III.6 (Points critiques de l'exponentielle)**.** Développement On note $F(T) = T^{-1}(1 - e^{-T})$. Pour $X \in M_n(\mathbb{C})$,

$$Dexp(X) = e^X.F(ad_X),$$

où $ad_X \in L(M_n(\mathbb{C}))$ et $ad_X.M = XM - MX$.

$$Dexp(X) \text{ non inversible} \Leftrightarrow \exists \lambda, \mu \in Spec(X), \lambda - \mu \in 2i\pi\mathbb{Z}^*.$$

Applications III.7. L'application $U_n(\mathbb{C}) \times H_n(\mathbb{C}) \to GL_n(\mathbb{C})$ est un $\mathbb{C}^\infty$-difféomorphisme.

IV Anneaux complets

[A completer]

V Développements

- Points critiques de l'exponentielle matricielle.
- Factorialité de $A[[X]]$.
- Dénombrement des solutions de $\{\alpha_1 p_1 + \cdots + \alpha_k p_k = n\}$.

VI Exercices

Exercice .1 (Calais Chap 7 Ex 1)**.** Montrer que $X^2 + 3X + 2$ est irréductible dans $\mathbb{Z}[[X]]$, mais pas dans $\mathbb{Z}[[X]]$.

Démonstration. On a $X^2 + 3X + 2 = (X + 1)(x + 2)$, donc $X^2 + 3X + 2$ n'ast pas irréductible dans $\mathbb{Z}[X]$. Si $X^2 + 3X + 2 = P(X)P(X)$ dans $\mathbb{Z}[[X]]$, alors $a_0(P)a_0(Q) = 2$, donc soit $a_0(P) \in \mathbb{Z}^\times$ soit $a_0(Q) \in \mathbb{Z}^\times$. □

Exercice .2 (Calais Chap 7 Ex 1)**.** (Corps des fractions) Soit A un anneau intègre, $A^* = A \setminus \{0\}$ et K son corps des fractions. Montrer que les conditions suivantes son équivalentes :

1. $K[[X]] = A[[X]][(A^*)^{-1}]$ (le localisé de $A[[X]]$ par (A^*)).
2. $K((X)) = Frac(A[[X]])$.
3. $\forall (a_n)_{n\in\mathbb{N}} \in A^{*\mathbb{N}}, \bigcap_{n\in\mathbb{N}} (a_i) \neq (0)$.

Démonstration. On a clairement les inclusions suivantes $A[[X]][(A^*)^{-1}] \subset K[[X]]$ et $Frac(A[[X]]) \subset K((X))$.

Supposons (1), alors comme $A[[X]][(A^*)^{-1}] \subset Frac(A[[X]])$, on en déduit que $K((X)) = Frac(K[[X]]) \subset Frac(A[[X]])$, d'où (2).

Supposons (2). Soit $(a_n)_{n\in\mathbb{N}} \in A^{*\mathbb{N}}$. On pose

$$F(X) = \sum_{n=0}^{+\infty} \frac{1}{a_0 \dots a_n} X^n \in K[[X]].$$

Alors l'hypothèse (2) montre qu'il existe $B(X), C(X) \in A[[X]]$ tels que $F(X) = \frac{B(X)}{C(X)}$. Comme $val(F(X)) = 0$, on peut prendre $B(X)$ et $C(X)$ tels que $val(B) = val(C) = 0$. On a alors

$$\forall n \in \mathbb{N}, c_n = \sum_{p+q=n} \frac{b_p}{a_0 \dots a_q}$$

On en déduit que $(a_0 \dots a_n)d_n = b_0 + b_1.a_n + b_1.a_{n-1}.a_n + \cdots + b_n.a_1 \dots a_n$, puis que $b_0 \in (a_m)$. D'où (3).

Supposons (3). Soit $F(X) = \sum_{n=0}^{+\infty} \frac{a_n}{b_n} X^n \in K[[X]]$. Soit $x \in \bigcap_{n\in\mathbb{N}} (b_n) \setminus \{0\}$ et $c_n \in A$ tel que $x = c_n.b_n$. On a alors $F(X) = x^{-1} \sum_{n=0}^{+\infty} c_n.a_n X^n$.

□

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

Références [Tauvel], [Arnaudies 1].

I Structure de $K(X)$

• I.A Définition

Définition I.1 (Corps des frations frationels)**.** L'espace $K(X)$ est l'ensemble des couples (P,Q) de $K[X]\times K[X]^*$, quotienté par la relation

$$(P,Q)\sim(P',Q')\iff PQ'=P'Q.$$

On note P/Q la classe de (P,Q).

Proposition I.2. Munie des lois $P/Q+P'/Q'=(PQ'+P'Q)/(QQ')$ et $P/Q.P'/Q'=(PP')/(QQ')$ (bien définies), $K(X)$ est un corps contenant $K[X]$, et tout corps contenant $K[X]$ contient $K(X)$.

Tout éléments de $K(X)$ possède une écriture P/Q avec $pgcd(P,Q)=1$, que l'on appelle irréductible, et elle est unique à association près.

Définition I.3 (Zéros et pôles)**.** Soit $F=P/Q$ sousforme irréductible. Les zéros de F sont les zéros de P et les pôles de F sont les zéors de Q.

• I.B Propriétés de $K(X)$

Définition I.4. Le degré de P/Q est $\deg(P/Q)=\deg P-\deg Q$ (non nécéssairement sous-forme irréductible).

Proposition I.5 (Propriété fonctiorielle)**.** Soit A une K-algèbre. Alors on a un isomorphisme $Hom_K(K(X),A)=\{\text{transcendants de } A\}$.

Applications I.6. ???

Proposition I.7. On a $\deg(F+G)\leq\max(\deg F,\deg G)$, et $\deg FG=\deg F\deg G$.

Applications I.8. $K(X)$ n'est pas clos.

• I.C Fonctions rationnels sur $\mathbb{R}$

Si x n'est pas pôle de $P(X)/Q(X)$, on peut définir $P(x)/Q(x)$.

Proposition I.9. Soit $F\in\mathbb{R}(X)$.
- Si y est pôle de F, alors $\lim_{y\to x}F(x)=\infty$.
- $\deg f<0$ si et seulement si $\lim_{x\to\pm\infty}F(x)=0$

Exemple I.10. ???

Applications I.11. ???

II Décomposition en éléments simples

• II.A Théorème

Définition II.1. Un *élément simple* est une fraction du type P/Q^n, avec Q un irréductible de $K[X]$ non constant et P de degré $\leq\deg Q-1$.

Dans une corps clos, les éléments simples sont du type $a/(X-b)^n$.

Théorème II.2. Toute fration rationelle s'écrit de façon unique comme somme d'un polynôme et d'éléments simples.

Corollaire II.3. $K(X)$ admet pour base $(X^n)_{n\in\mathbb{N}}\cup(X^k/Q^n)_{k\leq\deg Q}$.

Exemple II.4. Dans $\mathbb{C}(X)$, si $P(X)=\prod_{i=1}^{p}(X-r_i)^{n_i}$, alors la décomposition en éléments simples de P'/P est $\sum n_i/(X-r_i)$.

Applications II.5. Théorème de Guass-Lucas.

Applications II.6. Développement Déterminant de Cauchy et théorème de Müntz.

• II.B Décomposition pratique sur $\mathbb{R}$ et $\mathbb{C}$

Dans $\mathbb{C}$ les éléments simples sont du type $a/(X-r)^n$.
Méthodes pour les pôles d'ordre 1 :...
Méthodes pour les pôles d'ordre n :...

Applications II.7. Primitivation des fraction rationnelles : primitive des éléments simples...

[A completer]

III Théorème des résidues

IV Homographies

• IV.A Suites homographiques

• IV.B Homogrpahies de la droite complexe

V Liens avec les séries formelles

VI Développements

- Dénombrement des solutions d'une équation diophantienne
- Déterminant de Cauchy et théorème de Müntz.
- Automorphsime de $K(X)$.

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

Références [Chambert-Loir], [Goblot].

I Algèbre commutative sur $k[X]$

• I.A Polynômes irréductibles

Soit K un corps. On rappelle le $K[X]$ est un anneau euclidien.

Définition I.1. Un polynôme est *irréductible* s'il est non inversible et n'a pas de dviseur non trivial.

Exemple I.2.
- Tout polynôme de degré 1 est irréductible.
- Tout polynôme de degré ≤ 3 qui n'as pas de racine est irréductible.
- Tout polynôme de degré ≥ 2 admettant une racine n'est pas irréductible.
- $X^4 - 2$ est irréductible sur $\mathbb{Q}[X]$.

Proposition I.3. Pour $P(X) \in k[X]$, $P(X)$ est irréductible si et seulement si $k[X]/P$ est un corps.

Théorème I.4. $k[X]$ est factoriel : tout polynôme se décompose de façon unique (modulo inversible) en produit de polynôme irréductible.

Définition I.5. Un corps k est *clos* si les seuls irréductibles de $k[X]$ sont les polynômes de degré 1.

Théorème I.6. Développement [D'Alambert-Gauss] Le corps $\mathbb{C}$ est clos.

Corollaire I.7. Les irréductibles de $\mathbb{R}$ sont du type $X - a$ et $X^2 + bX + c$ avec $b^2 - 4c < 0$.

Applications I.8.
- Tout endomorphisme sur $\mathbb{C}^n$ est trigonalisable.
- Décompoistion en éléments simples.

Applications I.9. Si $P(X) \in \mathbb{R}[X]$ est positif si et seulement si c'est une somme de deux carrés.

• I.B Irréductibilité dans $\mathbb{Q}[X]$

Proposition I.10. Un polynôme unitaire de $\mathbb{Z}[X]$ est irréductible sur $\mathbb{Z}[X]$ si et seulement s'il est sur $\mathbb{Q}[X]$.

Théorème I.11. Soient p premier et $P(X) \in \mathbb{Z}[X]$ unitaire. Si $P(X) \mod p$ est irrédctible dans $\mathbb{F}_p[X]$, alors $P(X)$ est irréductible dans $\mathbb{Z}[X]$.

Exemple I.12.
- $X^2 - 7X + 21$ est irréductible modulo 2.
- $X^4 + 1$ est rédutible dans tous les $\mathbb{F}_p$.

Théorème I.13 (Critère d'Eisenstein)**.** Soient p premier et $P(X) \in \mathbb{Z}[X]$ de degré n. Si $P \mod p = aX^n \neq 0$ et si $p^2 \nmid P(0)$, alors P est irréductible sur $\mathbb{Z}[X]$.

Exemple I.14.
- Φ_p est irréductible pour p premier.
- ???

Proposition I.15. Développement Φ_n est irréductible pour tout n.

II Extensions de corps

• II.A Définitions et propriétés

Définition II.1. Soit k un corps. Une extension de k est un corps L munie d'une injection de corps $k \to L$. Auquel cas L est un k espace vectoriel. L'extension est dite finie si L est un k-espace vectoriel de dimension finie. On note $[L : k] = \dim_k L$.

Exemple II.2. $\mathbb{R}/\mathbb{Q}$, $(k[X]/P)/k$, ...

Proposition II.3. Si M/L et M/k sont des extensions finis, alors M est une extension finie de k et $[M : k] = [M : L].[L : k]$.

Corollaire II.4. tout corps fini est de cardinal p^n, avec $p = caract(k)$.

• II.B Corps de rupture et corps de décomposition

Définition II.5. Soit $P \in k[X]$ irréductible. Un corps de *rupture* de k est une extension L de k telle que $P(X)$ admette une racine et telle que L soit minimal pour cette propriété.

Exemple II.6.
- $\mathbb{C}$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$.
- $\mathbb{Q}[\sqrt[3]{2}]$ et $\mathbb{Q}[j\sqrt[3]{2}]$ sont deux corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.
- $k[X]/P$ est un corps de rupture de P sur k.

Théorème II.7 (Propriété fonctoriel)**.**
- Le corps de rupture est unique à isomorphisme de k-extension près.
- Si L est un corps, alors l'application $\begin{array}{ccc} k[X]/p & \longrightarrow & \{z \in L : P(z) = 0\} \\ f & \longmapsto & f(X) \end{array}$ est une bijection.

Exemple II.8. ???

Applications II.9. ???

Définition II.10. Soit $P \in k[X]$ irréductible. Un corps de décomposition de $P(X)$ est une extension L de k tel que $P(X)$ soit simplement scindé et tel que L soit minimal pour cette porprité.

Exemple II.11. ???

Théorème II.12. Il n'y a q'un seul corps de décomposition à isomorphisme près (l'isomorphisme est non canonique).

Théorème II.13. Tout corps admet une clôture algébrique unique à isomorphisme près (l'isomorphisme est non canonique).

III Polynômes sur les corps finis

• III.A Irréductibles en corps fini

Soit k un corps de cardinal $q = p^r$.

Théorème III.1. La décomposition en irréductible de $X^{q^n} - X$ est $X^{q^n} - X = \prod_{d|n} \prod_{P \in I(d,q)} P(X)$, où $I(d,q)$ est l'ensemble des irréductibles de $k[X]$ de degré d.

Théorème III.2. Il n'existe qu'un seul corps de cardinal q et c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Corollaire III.3. Si $P \in \mathbb{F}_p[X]$ est irréductible, alors son corps de rupture est aussi son corps de décomposition.

• III.B Factorisation de polynômes en corps fini

Proposition III.4. Développement [Algorithme de Berlekamp] ...

• III.C Application aux codes correcteurs cycliques

...

IV Applications aux nombres constructibles

• IV.A Construction à la règle et au compas

Définition IV.1. Soit Σ une partie de $\mathbb{C}$. Un nombre $z \in \mathbb{C}$ est dit *construtible* à la règle et au compas à partir de Σ si il existe une suite $P_1, \dots, P_n$ telle que

- $z = P_n$.
- Pour tout $i \leq n$, P_i est intersection de droites passant par deux points de $\Sigma_{i-1} := \Sigma \cup \{P_1, \dots, P_{i-1}\}$ ou de cercles centré en un point de Σ_{i-1} passant par un point Σ_{i-1}.

On note C_Σ leur ensemble.

Si $\Sigma \subset \mathbb{R}$, un réel est dit constructible à partir de Σ si c'est l'abcisse d'un point constructible sur $\mathbb{C}$.

Proposition IV.2. Si x est un nombre constructible à partir de $\mathbb{Q}$, alors x est algébrique et son polynôme minimal est irréductible.

Théorème IV.3. Développement [Wantzel, 1837] Soit $\Sigma \subset \mathbb{R}$ contenant $\{0,1\}$ et E le sous-corps de R qu'il engendre. Un réel x est constructible à partir de Σ si et seulement s'il existe une suite de sous-corps de $\mathbb{R}$

$$E = E_0 \subset E_1 \subset \cdots \subset E_n$$

telle que

- $x \in E_n$.
- $\forall i \in [i,n], [E_i : E_{i-1}] = 2$.

Corollaire IV.4.

- Un nombre constructible est de degré une puissance de 2 sur le corps de départ.
- $\sqrt[3]{2}$ n'est pas constructible sur $\mathbb{Q}$.
- L'angle $\alpha/3$ est constructible si et seulement si $X^3 - 3X + 2\cos(\alpha)$ n'est pas irréductible sur $\mathbb{Q}$.

Remarque IV.5. La réciproque est fausse : les racines de $X^4 - X - 1$ ne sont pas constructibles [CL, Alg. Corp., Exe 1.16].

Théorème IV.6. Un complexe $z \in \mathbb{C}$ est constructible si et seulement si le corps de décomposition de son polynôme minimal est une puissance de 2.

• IV.B Groupes de Galois

[A completer]

Théorème IV.7. Développement $\mathfrak{S}_p$ est un groupe de Galois sur $\mathbb{Q}$.

• IV.C Polygônes constructibles

Théorème IV.8 (Gauss)**.** Les n-gones constructibles sont les n tel que n est le produit d'une puissance de 2 et de nombres de fermat premiers distincts.

V Développements

- (...)

Exercice .1 (Chambert-Loir, Alg. Corp, Ex 1.6)**.** Soit $(p_i)_{i\in\mathbb{N}}$ des nombres premiers distincts. Pour $n \in \mathbb{N}$, on considère les assertions suivantes.

1. (a_n) L'extension $Q[\sqrt{p_1}, \dots, \sqrt{p_n}]$ est de degré 2^n sur $\mathbb{Q}$.
2. (b_n) Pour tout $x \in \mathbb{Q}$: x est un carré dans $Q[\sqrt{p_1}, \dots, \sqrt{p_n}]$ si et seulement s'il existe $I \subset [1,n]$ tel que $x \prod_{i\in I} p_i$ soit un carré dans $\mathbb{Q}$.

Montrer que pour tout $n \in \mathbb{N}$,

$$(a_n) \wedge (b_n) \Longrightarrow a_{n+1} \text{ et } b_n \wedge a_{n+1} \Longrightarrow b_{n+1}.$$

En déduire que $(\sqrt{p})_{p \text{ premier}}$ et une famille libre sur $\mathbb{Q}$.

Démonstration. Soit $n \in \mathbb{N}$.

Supposons (a_n) et (b_n). En prenant $x = p_{n+1}$, il n'existe pas de $I \subset [1,n]$ tel que $x\prod_{i\in I} p_i$ soit un carré dans $\mathbb{Q}$. Donc p_{n+1} n'est pas un carré dans $Q[\sqrt{p_1},\dots,\sqrt{p_n}]$. D'où (a_{n+1}).

Supposons (b_n) et (a_{n+1}). Si on note $K = \mathbb{Q}[\sqrt{p_1},\dots,\sqrt{p_n}]$, alors on a d'après (a_{n+1}), $Q[\sqrt{p_1},\dots,\sqrt{p_{n+1}}] = K \oplus K\sqrt{p_{n+1}}$ (y réfléchir). Soit $x \in \mathbb{Q}$. Si x est un carré dans $K[\sqrt{p_{n+1}}]$, alors x s'écrit $x = b^2$ avec $b = \alpha + \beta\sqrt{p_{n+1}} \in K \oplus K\sqrt{p_{n-1}}$ et $\alpha = 0$ ou $\beta = 0$.

- Si $\alpha = 0$, alors $x = \beta^2 p_{n+1} \in \mathbb{Q}$. D'après (b_n) appliqué à xp_{n+1}, il existe $J \subset [1,n]$ tel que $(xp_{n+1})\prod_{j\in J} p_j$ soit un carré dans $\mathbb{Q}$. On prend alors $I = J \cup \{p_{n+1}\}$.
- Si $\beta = 0$, alors $x = \alpha^2$. D'après (b_n), il existe $J \subset [1,n]$ tel que $x\prod_{j\in J} p_j$ soit un carré dans $\mathbb{Q}$. On prend alors $I = J$.

Réciproquement, s'il existe $I \subset [1,n]$ tel que $x\prod_{i\in I} p_i = y^2$ avec $y \in \mathbb{Q}$. Alors $x = \left(y\sqrt{\prod_{i\in I} p_i}\right)^2$ est un carré dans $K[\sqrt{p_{n+1}}]$. □

Exercice .2 (Chambert-Loir, Alg. Corp, Ex 1.7)**.** Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ tel que $|a_0| > \sum_{k=1}^{n} |a_k|$. Montrer que $P(X)$ est irréductible.

Démonstration. .[A completer] □

Exercice .3 (Chambert-Loir, Alg. Corp, Ex 1.8)**.** Soit $P(X) = X^n + \sum_{k=0}^{n-1} a_k X^k$ tel que $|a_{n-1}| > 1 + \sum_{k=2}^{n-2} |a_k|$. Montrer que $P(X)$ est irréductible.

Démonstration. .[A completer] □

117 - Algèbre des polynômes à n indéterminées. Polynômes symétriques. Applications

Références [Gob96], [Gou94].

I Structure de $A[X_1, \dots, X_n]$

• I.A Définitions et propriétés fondamentales

Définition I.1. Soit A un anneau commutatif et $n \in \mathbb{N}$. On définit par induction : $A[X_1, \dots, X_n] = A[X_1, \dots, X_{n-1}][X_n]$.

L'espace $A[X_1, \dots, X_n]$ est une A-algèbre commutative et est intègre si A est intègre. Pour polynôme $P \in A[X_1, \dots, X_n]$ s'écrit de façon unique en : $P = \sum_\alpha a_\alpha X^\alpha$, où la somme est à support fini, a_α et α parcourt l'ensemble des n-uplets de $\mathbb{N}$. On note $|\alpha|$ la taille de α.

Remarque I.2. On a isomorphisme canonique : $A[X][Y] \to A[Y][X]$ qui envoie X sur X et Y sur Y.

Définition I.3. Soit $P(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$. Le *degré total*, de p est $\deg P = max\{|\alpha| : a_\alpha \neq 0\} \in \mathbb{N}$. Pour $i \in [1, n]$ le *degré partiel* P par rapport à X_i est $\deg_{X_i} P = \max\{\alpha_i : a_\alpha \neq 0\}$.

Proposition I.4. Pour $P, Q \in A[X_1, \dots, X_n]$, on a
- $\deg(P + Q) \leq \max(\deg P, \deg Q)$, avec égalité si $\deg P \neq \deg Q$.
- $\deg(PQ) = \deg P \deg Q$.

Proposition I.5.
- A noethérien $\Rightarrow A[X_1, \dots, X_n]$ noethérien.
- Théorème de transfert : A factoriel $\Rightarrow A[X_1, \dots, X_n]$ factoriel.

Remarque I.6. Pour k corps, $k[X_1, \dots, X_n]$ n'est jamais principal si $n \geq 2$.

Proposition I.7 (Propriété fonctionnelle)**.** Soit R une A-algèbre commutative, et $x_1, \dots, x_n \in R$. Alors il existe un unique morphisme de A-algèbre de $A[X_1, \dots, X_n] \to R$ qui envoie X_i sur x_i.

Définition I.8. Pour $P(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$, la *fonction polynomiale* associée à $P(X_1, \dots, X_n)$ est $\begin{array}{ccc} A^n & \longrightarrow & A \\ (x_1, \dots, x_n) & \longmapsto & P(x_1, \dots, x_n) \end{array}$.

Proposition I.9. Pour $x_1, \dots, x_n \in A$, l'application

$$Ev_x : \begin{array}{ccc} A[X_1, \dots, X_n] & \longrightarrow & A \\ P(X_1, \dots, X_n) & \longmapsto & \mapsto \ P(X_1, \dots, X_n) \end{array}$$

est un morphisme de A-algèbre.

• I.B Polynômes homogènes

Définition I.10.
- Un monôme est un polynôme du type X^α.
- Un *polynômes homogènes* de degré n est un polynôme dont tous le monômes sont de degré n. Le polynôme nul est homogène de degré n pour tout n. On note $A_n[X_1, \dots, X_p]$ leur ensemble.

Proposition I.11. L'algèbre des polynôme est graduée :

$$A[X_1, \dots, X_n] = \bigoplus_{d=0}^n A_n[X_1, \dots, X_p].$$

Proposition I.12. Pour $P, Q \in k[X_1, \dots, X_p]$, le produit PQ est homogène si et seulement si P et Q sont homogènes.

Proposition I.13. Un polynôme $P(X_1, \dots, X_p)$ est homogène de degré d si et seulement si $P(\lambda X_1, \dots, \lambda X_p) = \lambda^d P(X_1, \dots, X_p)$.

II Polynômes symétriques et antisymétriques

• II.A Action de $\mathfrak{S}_n$ sur $A[X_1, \dots, X_n]$

Proposition II.1. Le groupe $\mathfrak{S}_n$ agit à gauche sur $A[X_1, \dots, X_n]$ par automorphisme de A-algèbre en permutant les indéterminées.

Définition II.2. Un polynôme P est dit *symétrique* s'il est invariant par $\mathfrak{S}_n$, et *antisyméytrique* si : $\forall \sigma \in \mathfrak{S}_n, \sigma.P = \varepsilon(\sigma)P$.

Proposition II.3.
- P est symétrique si et seulement si pour toute transpositions τ, $\tau.P = P$.
- P est antisymétrique si et seulement si pour toute transpositions τ, $\tau.P = -P$.

Exemple II.4.
- Vandermonde : le polynôme $V = \prod_{i<j}(X_i - X_j)$ est antisymétrique.
- ? ? ?

• II.B Polynômes symétriques élémentaires

Définition II.5. On muni $\mathbb{N}^n$ de l'ordre lexicographique (c'est alors un ensemble bien ordonné). Le *degré lexicographique* de P est $\deg_{lex} P = \max_{lex}\{\alpha : a_\alpha \neq 0\}$.

Proposition II.6. Pour $P, Q \in A[X_1, \dots, X_n]$, on a
- $\deg_{lex}(P + Q) \leq \max(\deg_{lex} P, \deg_{lex} Q)$, avec égalité si $\deg_{lex} P \neq \deg_{lex} Q$.
- $\deg_{lex}(PQ) = \deg_{lex} P \deg_{lex} Q$.

Définition II.7. On note pour $k \in [1, n]$, $\sigma_k = \sum_{i_1 < \dots < i_k} X_{i_1} \dots X_{i_k}$ le k^{em} *polynôme symétrique élémentaire.*

Proposition II.8.
- Les σ_k sont des polynômes symétriques.

– Le degré lexicographique de $\sigma(k)$ est $(1,\dots,1,0,\dots,0)$. Le degré de $\sigma_{k_1}\sigma_{k_2}\dots\sigma_{k_p}$ est $(\overbrace{p,\dots,p}^{k_1},\underbrace{p-1,\dots,p-1}_{k_2},\dots)$.

Théorème II.9. L'application $\begin{array}{ccc} A[\Sigma_1,\dots,\Sigma_n] & \longrightarrow & Sym(A[X_1,\dots,X_n]) \\ \Sigma_i & \longmapsto & \sigma_i \end{array}$ est un isomorphisme.

Remarque II.10. Pour trouver la bijection réciproque on regarde le degré lexicographique. (Algorithme de ? ?)

Théorème II.11. L'application $\begin{array}{ccc} Sym(k[X_1,\dots,X_n]) & \longrightarrow & Asym(k[X_1,\dots,X_n]) \\ P & \longmapsto & V.P \end{array}$ est un isomorphisme.

Applications II.12. Si $K \subset L$, $P(X) \in K[X]$ et si $Q(X) \in L[X]$ est telle que ses coefficients sont symétrique en les racines de $P(X)$, alors $Q(X) \in K[X]$.

• II.C Relations coefficients-racines et sommes de Newton

Proposition II.13. On a $\prod(T - X_i) = \sum_{k=0}^{n}(-1)^k\sigma_k T^{n-k}$.

Corollaire II.14. Pour $P(X) = a_dX^d + \dots + a_0 \in k[X]$ et $z_1,\dots,z_d \in \overline{K}$ ses racines on a : $\frac{a_{d-k}}{a_d} = (-1)^k\sigma_k(z_1,\dots,z_d)$.

Applications II.15. Développement Action de $\mathbb{C}[X_{i,j}]$ sur $\mathcal{M}_n(\mathbb{C})$ [A completer].

Définition II.16. On note pour $k \in [0,n]$, $S_k = X_1^k + \dots + X^n$, la k^{em} somme de Newton.

Proposition II.17.
– S_k est un polynôme symétrique.
– Pour $k \in [1,n]$, on a : $\sum_{p+q=k} S_p(-1)^q\sigma_q + (-1)^k k\sigma_k = 0$. Cette formule permet d'exprimer les S_k en fonction des σ_k et inversement.
– Pour $k \geq n+1$, on a : $\sum_{p+q=k, q\leq n} S_p(-1)^q\sigma_q = 0$.

Applications II.18.
– Soit M tel que $\forall n \in \mathbb{N}, Tr(M^n) = 0$, alors M est nilpotent.
– ? ? ?

• II.D Discriminant

Définition II.19. Le *discriminant* est $Disc_n = A_n^{2n-2}\prod_{i<j}(X_i - X_j)^2$.

Proposition II.20. $Disc_n$ est un polynôme symétrique homogène de degré $2n-2$.

Donc $Disc_n$ est un polynôme en les $A_k = A_n\sigma_k$.

Exemple II.21.
– $Disc_2 = A_2^2(X_1 - X_2)^2 = (A_2\sigma_1)^2 - 4A_2^2\sigma_2$.
– Si $P(T) = P = X^3 + pX + q$,alors $Disc(P) = -4p^3 - 27q^3$.

Applications II.22. Soit $P = aX^2 + bX + c \in \mathbb{R}[X]$.
– Si $b^2 - 4ac > 0$, alors P a deux racines réelles distinctes.
– Si $b^2 - 4ac = 0$, alors P a une racine réelle double.
– Si $b^2 - 4ac < 0$, alors P a deux racines complexes conjugué.

Applications II.23. Soit $P = X^3 + pX + q \in \mathbb{R}[X]$.
– Si $-4p^3 - 27q^2 > 0$, alors P a trois racines réelles distinctes.
– Si $-4p^3 - 27q^2 = 0$, alors P a trois racines réelles dont une double (éventuellement triple).
– Si $-4p^3 - 27q^2 < 0$, alors P a une racine réelle et deux racine complexe conjugué.

Exemple II.24. ? ? ?

III Application à la géométrie algébrique

• III.A Variétés algébriques

Définition III.1. Soit I un idéal de $\mathbb{R}[X_1,\dots,X_n]$. La *variété algébrique* associé est I est $V(I) = \{x \in \mathbb{R}^n \mid \forall P \in I, P(x) = 0\}$.

Proposition III.2. Si un polynôme s'annule sur un ouvert, alors c'est le polynôme nul.

Corollaire III.3. Une variété algébrique différente de $\mathbb{R}^n$ est d'intérieur vide.

Théorème III.4 (Nullstellensatz)**.** ...

Corollaire III.5. Si I est un idéal strict, alors $I \neq \emptyset$.

Théorème III.6. Développement [Bezout faible]...

IV Applications aux extensions de corps

Définition IV.1 (degré de transcenance)**.**

[A compléter]
Théorème de Schur

V Développements

– Théorème de Bezout.
– Action du groupe alterné sur $k[X_1,\dots,X_n]$.
– Théorème de Chevalley-Warning.
– Théorème de Schur/Burnside.

VI Exercices

Exercice .1 (Gourdon Chap 1.1 Ex 6)**.** Soit $P \in \mathbb{Z}[X]$ unitaire et $r \in \mathbb{Q}$ racine rationnelle de P. Montrer que r est entier.

Démonstration. Si $r = a/b$ est sous forme irréductible. Alors $b^{\deg p} \cdot P(a/b)$ vaut 0 et est congrue à $a^{\deg P} \mod b$. Comme a est premier avec b celà implique $b = 1$. □

118 - Exemples d'utilisation de la notion de dimension en algèbre et en géométrie

Références [...]

Introduction [A compléter]

I Dimension d'un espace vectoriel

• I.A Algèbre linéaire

Définition I.1. Une base est une famille libre et générqtrice.

Proposition I.2. Toute espace vectoriel admet une base, et deux bases admettent le même cardinal.

Définition I.3. La *dimension* d'un espace vectoriel est le cardinal d'une base.

Proposition I.4. Deux espaces vectoriels sont isomorphes si et seulement si ils ont la même dimension.

Proposition I.5.
- $\dim E \times F = \dim E + \dim F$.
- $\dim L(E,F) = \dim E \times \dim F$.

Proposition I.6. Si E et F sont seux sous-espaces de dimension finie et si $E \subset F$ alors $E = F$.

Proposition I.7 (Grassmann)**.** En dimension finie : $\dim E + F = \dim E + \dim F - \dim E \cap F$.

Applications I.8. Théorème de Silvester : la signature d'une forme quadratique réel est unique.

• I.B Propriétés en dimension finie

Proposition I.9. Si $f :\to E$ est un endomorphisme de E, alors
- $codim(\ker f) = rg(f)$.
- f est bijective $\iff$ f est surjective $\iff$ f est injective.

Cas réel

Théorème I.10. Toutes les normes sur un $\mathbb{R}$-espace vectoriel de dimension finie sont équivalentes.

Théorème I.11 (Continuité automatique)**.** Toute application linéaire est continue.

Théorème I.12 (Dualité)**.** Soit E un espace vectoriel de dimension finie.
- E est réflexif.
- Si E est euclidien, alors E est canoniquement isomorphe à E^*.

Théorème I.13. En dimension finie dans un coprs clos, tout endomorphisme admet une valeur propre et est trigonalisable.

• I.C Espaces affines

Définition I.14. Un espace est en ensemble munie d'une action simplement transitive d'un $\mathbb{R}$-espace vectoriel.

Théorème I.15 (Carathéodory)**.** Dans un espace affine de dimension n, l'enveloppe convexe de A est l'ensemble des barycentres de $n+1$ points de A.

II Extensions de corps

• II.A Degré d'extension et extensions Galoisiennes

[A completer]

• II.B Nombres constructibles

[A completer]

III Topologie de $\mathbb{R}^n$

• III.A Calcul différentielle

[A completer]

• III.B Sous-variétés

[A completer]

IV Développements

–

119 - Exemples d'actions de groupes sur les espaces de matrices

Références [...]

Introduction [A compléter]

I Représentation linéaires de groupes finie

• I.A Définition

• I.B Caractères

II Classes d'équivalences et de similitudes

• II.A Matrices semblables

Soit A un anneau.

Définition II.1. La groupe $GL_n(A) \times GL_n(A)$ agit sur $M_n(A)$, par $(g,h)M = gMh^{-1}$. Deux matrices dans une même orbites sont dites équivalentes.

Proposition II.2. Si A est un corps, alors deux matrices sont équivalentes si et seulements si elles ont le même rang.

Exemple II.3. ? ? ?

Théorème II.4 (Diviseurs élémentaires)**.** Si A est un anneau principal, alors les matrices $diag(d_1, d_2, \ldots, d_n)$, avec $d_1|d_2|\cdots|d_n$ forment un système de représentants des classe d'équicalence.

Exemple II.5. ? ? ?

• II.B Matrices équivalentes et réduction

Définition II.6. Le groupe $GL_n(A)$ agit sur $M_n(A)$ par conjugaison. Les orbites sont appelées classes de similitudes de $M_n(A)$.

Proposition II.7. Si deux matrices ont semblables, alors elles ont même déterminant, trace, polynôme caractéristique.

Exemple II.8. ? ? ?

Théorème II.9 (Réduction de Jordan)**.**

Proposition II.10 (Topologie des classes de similitudes)**.**

• II.C Formes quadratiques et matrices congruentes

III Géométrie

IV Action du corps des quaternions

• IV.A Action du groupe modulaire sur le demi-plan de Poincaré

Définition et domaine fondamental. Classification des réseaux de $\mathbb{C}$.

V Développements

- Sous-groupes compacts de $GL_n(\mathbb{R})$.
- $PSU_2(\mathbb{C}) \simeq SO_3(\mathbb{R})$.
- $PSL_2(\mathbb{R}) \simeq O_0(2,1)$

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

Références [Arnaudies], [Escofier (alg. licence)].

I Structure des espaces vectoriels de dimension finie

• I.A Bases d'un espace vectoriel

Définition I.1. Soit k un corps commutatif et E un k-easpace vectoriel.
- Une famille fini $(x_i)_{i\in[1,n]}$ est *libre* s'il n'y a pas de relations de dépendance linéaire. Une famille infinie est *libre* si toute sous-famille finie est libre.
- Une famille $(x_i)_{i\in I}$ est *génératrice* si $vect(x_1,\dots,x_n) = E$.
- Une famille $(x_i)_{i\in I}$ est une *base* si elle est libre et génératrice.

Proposition I.2.
- Toute sous-famille d'une famille libre est libre.
- Toute sur-famille d'une famille génératrice est génératrice.
- Une famille libre est une base si et seulement si elle libre maximale. Une famille génétrice est une base si et seulement si elle est minimale.

Définition I.3. Un espace vectoriel est de dimension finie s'il elle admet une famille génératrice finie.

Théorème I.4 (Lemme de Steinitz)**.** Si $(e_i)_{i\in[1,n]}$ est une famille génératrice, alors toute famille de cardinal $n+1$ est liée.

Théorème I.5 (Théorème de la base incomplète)**.** Si e est une famille libre et f une famille génératrice, alors on peut compléter e en une base avec les éléments de f.

Applications I.6.
- Si $M \in \mathcal{M}_n(k)$ tel que $\forall N \in \mathcal{M}_n(K), \det(M+N) = \det M + \det N$, alors $M = 0$.
- ???

Corollaire I.7. Tout espace vectoriel de dimension finie admet une base et le cardinal de la base est unique.

Définition I.8. La *dimension* d'un espace vectoriel est le cardinal d'une base.

Exemple I.9.
- $K[X]$ a pour base $(1, X, \dots,)$ (infinie).
- Si X est un ensemble fini, alors $F(X,\mathbb{R})$ a pour base $(\delta_x)_{x\in X}$.
- ???

Applications I.10. Développement Sous-espaces de dimension finie de $C^0(\mathbb{R},\mathbb{R})$ stables par translation.

Proposition I.11. Tout espace vectoriel de dimension n est isomorphe à k^n.

Remarque I.12. On se ramène alors au calcul matricielle.

• I.B Sous-espace vectoriels d'un espace vectoriel de dimension finie

Proposition I.13. Un sous-espace vectoriel d'un espace vectoriel de dimension finie est lui-même de dimension finie.

Proposition I.14. Tout sous-espace vectoriel admet un supplémentaire. Si $F \oplus G = E$, alors $\dim F + \dim G = E$.

Applications I.15.
- Si μ_A est irréductible, alors A est semi-simple.
- Soit $f \in L(E)$, alors $f.L(E) = \{g : \operatorname{Im} g \subset \operatorname{Im} f\}$ et $L(E).f = \{g : \ker g \supset \ker f\}$

Proposition I.16 (Grassmann)**.** $\dim(F+G) = \dim F + \dim G - \dim F \cap G$.

Applications I.17.
- Théorème de Courant-Fisher : ...
- Signature d'une forme quadratique réelle : ...

Proposition I.18. Si $F \subset E$, et si $\dim F = \dim E$, alors $E = F$.

Corollaire I.19. Il n'existe pas de suite strictement décroissante d'espaces vectoriels. Donc on peut raisonner par récurrence sur la dimension.

Applications I.20.
- Toute famille commutative d'endomorphisme trigonalisable est cotrigonalisable.
- Développement [Lie-Kolchin] Soit E un $\mathbb{C}$-esapce vectoriel de dimension finie et G un sous-groupe connexe résoluble de $GL(E)$. Alors G est trigonalisable.

II Rang

• II.A Rang d'une famille de vecteurs

Définition II.1. Le rang d'une famille de vecteurs est la dimension du sous-espace qu'il engendre.

Proposition II.2.
- Une famille de cardinal n est une base $\iff$ elle est libre $\iff$ elle est de rang n.
- Si une famille à r éléments est de rang r, alors elle est base du sous-esapce qu'elle engendre.

• II.B Rang d'une application linéaire

Définition II.3. Le rang d'une application linéaire est la dimension de son image.

Proposition II.4.
- L'image d'une famille génératrice est une famille génératrice de l'image.
- L'image d'une famille lié est une famille liées.
- L'image d'une famille libre par une application injective est libre.

Théorème II.5 (du rang)**.** Pour $f : E \to F$, on a $\dim\ker f + rg(f) = \dim E$.

Proposition II.6. Pour f un endomorphisme : f est inversible $\iff$ f est inversible à gauche $\iff$ $f$est inversible à droite $\iff$ f est de rang n.

Applications II.7.
- Tout k-algèbre de dimension finie intègre est un corps.
- $E = E^{**}$.

• II.C Dualité en dimension finie

[A completer]

Théorème II.8 (Critère de nilpotence de Cartan)**.** .

III Topologie sur les espaces vectoriels réelles de dimension finies

• III.A Équivalence des normes

• III.B Continuité automatique

IV Extensions de corps

• IV.A Degré d'une extension et extensions Galoisiennes

• IV.B Nombres constructibles

V Développements

- Théorème de Lie-Kolchin.
- Critère de nilpotence de Cartan.
- Sous-espaces de dimension finie de $C^0(\mathbb{R}, \mathbb{R})$ stable par translation.
- Théorème de d'Alembert-Gauss.
- L'extension $\mathbb{Q}[\sqrt{p_1}, \dots]$.
- Théorème de Wantzel.
- Sur l'exponentiel matricielle.
- Théorème de Groethendick.
- Théorème de Weddderburn.
- Théorème d'Engel.

Exercice .1 (FGN, Alg ?)**.** Soit $F_1, \dots, F_p$ des espaces vectoriels de même dimension. Montrer qu'il existe un supplémentaire commun.

Démonstration. On prend G un sous espace tel que pour tout $i \in [1, p], F_i \cap G = 0$.
[A completer] □

121 - Matrices équivalentes. Matrices semblables. Applications.

Références [...]

I Notion d'équivalence et de similitude

• I.A Classes d'équivalence

Soit $\mathbb{A}$ un anneau principal.

Définition I.1. Deux matrices $A, B \in \mathcal{M}_{n,m}(\mathbb{A})$ sont *équivalents* si

$$\exists P \in GL_n(K), \exists Q \in GL_m(K), PAQ^{-1} = B.$$

C'est une relation d'équivalence sur l'ensemble $\mathcal{M}_{n,m}(\mathbb{A})$.
Celà s'interprète comme un changement de bases au départ et à l'arrivé.

Proposition I.2. Si $\mathbb{A}$ est un corps. deux matrices sont équivalentes si et seulement s'ils ont le même rang.

• I.B Opérations élémentaires sur les lignes et les colonnes

Définition I.3. Une matrice de *transvection* est une matrice de la forme

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

Une matrice de *dilation* est une matrice de la forme

$$diag(1, \dots, \lambda, \dots, 1).$$

La multiplication à gauche (resp. à droite) par ces matrices s'interprètent comme des opérations sur les lignes (reps. colonnes),
[A completer]

• I.C Classes de similitude

Définition I.4. Deux matrices $A, B \in \mathcal{M}_n(\mathbb{A})$ sont *semblables* si

$$\exists P, Q \in GL_n(K), PAP^{-1} = B.$$

Celà s'interprète par un changement de base sur les endomorphismes.
La classe de similitude d'un scalaire est réduit à un singleton.

Proposition I.5.
- Les éléments suivant sont invariants par similitude : trace, déteminant, polynôme minimale/caractéritique.
- Si $A = PBP^{-1}$, alors pour f un polynôme, on a $f(A) = Pf(B)P^{-1}$.

Théorème I.6. Si $A, B \in \mathcal{M}_n(\mathbb{R})$ sont semblables sur $\mathcal{M}_n(\mathbb{C})$, alors ils sont semblables sur $\mathcal{M}_n(\mathbb{R})$.

II Classification des classes équivalence et de similitude

• II.A Classe d'équivalence sur un corps

Proposition II.1. Deux matrices sont équivalentes si et seulement s'ils ont le même rang.

Applications II.2. Si q est une forme quadratique multiplicative non nulle sur $M_n(\mathbb{R})$, alors $n = 2$ et $q = \det$.

• II.B Théorème des diviseurs élémentaires

Théorème II.3 (Diviseurs élémentaires)**.** Soit $A \in \mathcal{M}_{n,m}A$. Alors il existe des matrices $P \in GL_nA$ et $P \in GL_mA$ et $d_1, \dots, d_n \in A$ tel que

$$PAQ = diag(d_1, \dots, d_n),$$

$$\text{et } d_1|d_2| \cdots |d_n.$$

Applications II.4. Réseaux et formes quadratiques [A completer].

Applications II.5. Les groupe abéliens de types finis sont produits de $\mathbb{Z}/n\mathbb{Z}$.

III Diagonalisation, trigonalisation et réduction

Soit K un corps.

Définition III.1. Une matrice est dite *diagonalisable* (resp. *trigonalisable*), si elle est semblable à uen matrice diagonale (resp. triangulaire).

Proposition III.2. Une matrce est diagonalisable (resp. trigonalisable) si et seulement si il existe un polynôme annulateur simplement scindé (resp. scindé)

Applications III.3. Si f est diagonalisable et si F est stable, alors $f_{|F}$ est diagonalisable.

Théorème III.4 (Décomposition de Frobenius)**.** .[A completer].

Corollaire III.5. Soit $K \subset L$.
- Si $M, N \in \mathcal{M}_n(K)$ sont semblables sur $\mathcal{M}_n(L)$, alors ils sont semblables sur $\mathcal{M}_n(K)$.
- Si $M \in \mathcal{M}_n(K)$, alors .

Théorème III.6 (Jordan)**.** [A completer].

Applications III.7. Toute matrice est semlable à sa transposée et on peut prendre la matrice de passage symétrique : i.e. si f est un endomorphisme, alors il existe une forme quadratique q non dégénérée telle que f soit autoadjoint pour q.

• **III.A Classes de similitudes sur $\mathcal{M}_n(\mathbb{R})$ et $\mathcal{M}_n(\mathbb{C})$**

IV Propriétés topologiques

Proposition IV.1. L'ensemble des matrices diagonalisables est dense dans les matrices trigonalisables.

Proposition IV.2. La classe de similitude d'une matrice est fermé si et seulement si elle est diagonalisable. Elle est bornée si et seulement si elle est sclaire.

V Réduction en espace euclidien

Proposition V.1. Les autoadjoints sont diagonalisables.

Proposition V.2. Les orthogonaux sont orthogonalement conjugué à $diag(1, ..., -1, R_\theta, ...)$.

VI Développements

- Théorème de Lie-Kolchin.
- Fonction polynômiales constantes sur les classes de similitudes.
- Sous-groupes compacts de $GL_n(\mathbb{R})$.
- Quadriques dans $M_2(\mathbb{R})$.
- Topologie sur les matrices.
- Théorème de Brauer.

123 - Déterminant. Exemples et applications

Références [AB], [Tau], [Gob96], [Gou94], [Escofier (alg. licence)].

I Définition et propriétés du déterminant

• I.A Formes n-linéaires alternées

Soient A un anneau commutatif, E un A-module libre de rang n et $(e_i)_{i\in[1,n]}$ une base.

Définition I.1. Une forme n-linéaire alternée sur M est une application de $f : E^n \to A$, linéaire par rapport à chaque variable et telle que $f(x_1, ..., x_n) = 0$ si $x_i = x_j$ pour un certain $i \neq j$. On note $\Lambda^n E$ leur ensemble.

Toute forme n-linéaire alternée est antisymétrique.

Proposition I.2. $\Lambda^n E$ est libre de rang 1 engendrée par. Si e est une base, alors il est engendré par $\det_e = \sum_\sigma \prod_{k=i}^n dX_i^{\sigma_i}$, qu'on appelle le déterminant dasn la base e.

Proposition I.3.
- Le déterminant ne change pas en remplaçant le vecteur x_i par $x_i + tx_j$.
- Si A est un **corps** alors le déterminant d'une famille liée est nulle.
- Si (e) et (f) sont deux bases alors $\det_e = \det_e(f) \det_f$.

• I.B Déterminant d'une matrice et d'un endomorphisme

Définition I.4. Si $M = [m_i^j] \in M_n(A)$, alors son déterminant est $\det M = \sum_\sigma \prod_{k=i}^n m_i^j$.

Si $(e_i)_{i\in[1,n]}$ est une base et (x_i), alors $\det_e(x_1, \dots, x_n) = \det Mat_e(x_1, \dots, x_n)$.

Proposition I.5. Le déterminant d'une matrice triangulaire est les produit de ces coefficients diagonaux.

Définition I.6. Si $f \in End(E)$. Alors f induit une application linéaire $\Lambda^n f : \Lambda^n E \to \Lambda^n E$. Comme $\Lambda^n E$ est de rang 1, c'est une homothétie et on note $\det f$ son rapport.

Proposition I.7. On a $\det f = \det Mat_e(f) = \det_e(f(e_1), \dots, f(e_n))$.

Proposition I.8.
- $\det(f.g) = \det f. \det g$.
- $\det(\lambda f) = \lambda^n \det f$

II Calcul de déterminants

• II.A Opérations sur les matrices et comatrice

Définition II.1. Soit M une matrice.
- Soient $I = (i_1, \dots, i_k)$ et $J = (j_1, \dots, j_k)$ deux k-uplet. Le mineur d'ordre (I, J) de M est $M(I, J) = \det[m_{i,j}]_{i\in I, j\in J}$.
- Cofacteurs d'indice (i_0, j_0) est $(-1)^{i+j} \det[m_{i,j}]_{i\neq i_0, j\neq j_0}$. La comatrice de M est la matrice des cofacteurs, noté ${}^tCom(M)$.

Proposition II.2. Soit $M \in \mathcal{M}_n(A)$. On a .

Définition II.3. Les *matrice de transvertions* sont les matrices de la forme $E_{i,j}(\lambda)$. Une *matrice de dilatation* est une matrice de la forme $D_i(\lambda) = diag(1, \dots, \lambda, \dots, 1)$.

Proposition II.4.
- On a $\det(M.E_{i,j}(\lambda)) = \det(E_{i,j}(\lambda).M) = \det M$.
- On a $\det(M.D_i(\lambda)) = \det(D_i(\lambda).M) = \lambda \det M$.

Théorème II.5. Soit A un anneau commutatif et $M \in \mathcal{M}_n(A)$.
- ${}^tCom(M).M = \det M I_n$
- M bijective $\iff$ M surjective $\iff$ $\det M$ inversible.
- M injective $\iff$ $\det M$ non diviseur de 0.

Applications II.6.
- Pour $M \in \mathcal{M}_n(\mathbb{Z})$: $M \in GL_n(\mathbb{Z}) \iff \det M = \pm 1$. Le volume d'un réseau de $\mathbb{R}^n$ est indépendante de la base.
- Les zéros de $\det(X - f)$ sont les valeurs propres de f.
- Deux polynômes sont premiers entre eux si et seulement si leur résultant est non nul.
- Formules de Cramer : Si A est inversible, alors $AX = B$ a pour solution : $x_i = \dfrac{\det(A_1, \dots, B, \dots, A_n)}{\det A}$.

Proposition II.7 (Déterminant par bloc)**.** Si $M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$, alors $\det M = \det A. \det D$.

Exemple II.8.
- Déterminant de Vandermonde.
- Développement [Formule de Gramm] Si $(e_1, \dots, e_n)$ est une famille libe un espace euclidien alors : $d(x, vect(e_1, ..., e_n)) = \dfrac{Gram(e_1, \dots, e_n, f)}{Gram(e_1, \dots, e_n)}$.

  [Déterminant de Cauchy] ...

  [Müntz] La famille $(X^{\alpha_n})_{n\in\mathbb{N}}$ est de vectoriel dense si et seulement si $\sum 1/\alpha_n$ diverge.

III Utilisation du déterminant en analyse et géométrie

• III.A Régularité de déterminant

Proposition III.1. Le détermiant est une application C^∞.

Applications III.2.
- $GL_n(\mathbb{R})$ n'est pas connexe.
- $GL_n(\mathbb{R})$ et $GL_n(\mathbb{C})$ sont des ouverts denses.
- L'application rang est semi continue inférieurement (Théorème du rang constant).
- L'inversion $M \mapsto M^{-1} = \det M^{-1\,t}Com(M)$ est C^∞.

• III.B Calcul de volumes

Proposition III.3. Soit $P = [0,1]e_1 + \cdots_[0,1]e_n$ u parallélépipède de $\mathbb{R}^n$. Alors sa mesure de Lebesgue est $\lambda_n(P) = \det(e)$, où le déterminant est prise dans la base canonique.

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie n et ω une forme n-linéaire alternée. On associe la mesure μ tel que pour tout parallélépipède $P = [0,1]e_1 + \cdots_[0,1]e_n$, on a $\mu(P) = \omega(e_1, \ldots, e_n)$.

Théorème III.4 (Mesure image)**.**
- Pour $A \in L(E)$ et X une partie mesurable, on a $\mu(A.X) = \det A.\lambda(X)$.
- Pour f un C^1-difféomorphisme : $f_*\mu = Jf^{-1}.\mu$.

Théorème III.5 (Inégalité d'Hadamard)**.** Soit E un espace vectoriel euclidien. L'espace E est alors munie de la mesure μ telle que pour toute base orthonormée, on a $\det([0,1]e_1 + \cdots + [0,1]e_n) = 1$. Pour toute famille $(x_1, \ldots, x_n)$, on a $\mu(x_1, \ldots, x_n) \leq \prod_{i=1}^n \|x_i\|$.

Définition III.6. On considère E un espace euclidien. Si $q \in Q^{++}(E)$ est une forme quadratique définie positive, alors l'*ellipsoïde* centré en 0 associée à q est l'ensemble

$$E_q = q^{-1}([0,1]).$$

- Son volume $Vol(q)$ est sa mesure de Lebesgue.
- Son déterminant est le déterminant de sa matrice dans une base orthonormée. C'est aussi le détermiant de $A \in S^{++}(E)$ son endomorphisme autoadjoint associé.

Théorème III.7. Développement [Ellipsoïde de John] Si K est un compact d'intérieur non vide, alors il existe une unique ellipsoïde de volume minimal contenant K.

Corollaire III.8. Tout sous-groupe compacts de $GL_n(\mathbb{R})$ est conjugué à un sous-groupe de $O_n(\mathbb{R})$.

• III.C Coordonnées barycentriques

On considère un plan affine E et (A, B, C) un repère.

Théorème III.9.
- Soient $X = (x_1, x_2, x_3)$, $Y = (y_1, y_2, y_3)$ et $Z = (z_1, z_2, z_3)$ trois points de E. Alors ls points (X, Y, Z) sont alignés si et seulement si $\det(X, Y, Z) = 0$.
- Soient $D_i : \alpha_i x + \beta_i y + \gamma_i z = 0$ $(i = 1, 2, 3)$, trois droites. Alors les trois droites (D_1, D_2, D_3) sont concourantes ou parrallèles si et seulement si $\det(\vec{\alpha}, \vec{\beta}, \vec{\gamma}) = 0$.

Applications III.10.
- Théorème de Ménélaus : soient $P \in (B, C)$, $Q \in (C, A)$ et $R \in (A, B)$ différents des sommets. Alors : P, Q, R sont alignés $\iff \frac{\bar{PB}}{\bar{PC}}.\frac{\bar{QC}}{\bar{QA}}.\frac{\bar{RA}}{\bar{RB}} = +1$.
- Théorème de Ceva : soient $P \in (B, C)$, $Q \in (C, A)$ et $R \in (A, B)$ différents des sommets. Alors : $(AP), (BQ), (CR)$ sont concourantes ou parralèles $\iff \frac{\bar{PB}}{\bar{PC}}.\frac{\bar{QC}}{\bar{QA}}.\frac{\bar{RA}}{\bar{RB}} = -1$.

IV Développements

- Sous-espaces stables de dimension finie de $C^0(\mathbb{R}, \mathbb{R})$ stables par translation.
- Ellipse de John.
- Déterminant de Gramm et théorème de Muntz.
- Theoreme de Frobenius-Zolotarev.
- Théorème de Pascal.
- Injective équivaut à déterminant non diviseur de 0.

Exercice .1. Montrer que $\det(A + x\phi) = \phi.{}^tCom(A)x + \det A$.

124 - Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications

Références [Gou94], [Gob95], [AB], [Escofier (alg. licence)], [Rombaldi].

I Polynôme d'endomorphismes

E désigne un espace vectoriel de dimension finie n sur un corps k commutatif.

Définition I.1. Pour $P = \sum_{k=0}^{n} a_n X^n \in k[X]$ et $f \in L(E)$, on note $P(f) = \sum_{n=0}^{n} a_n f^n$. On note $k[f]$ l'ensemble des polynômes en f.

Proposition I.2. Pour $f \in L(E)$, l'application $\begin{array}{ccc} k[X] & \longrightarrow & L(E) \\ P & \longmapsto & P(f) \end{array}$ est un morphisme de k-algèbre.

Définition I.3. Pour $f \in L(E)$, le *polynôme minimale* de f est le générateur unitaire de $\ker(P \mapsto P(f))$. On le note μ_f (différent de 0 car $L(E)$ est de dimension finie). Un *polynôme annulateur* de f est un élément du noyau.

Exemple I.4.
- Si f est un projecteur alors le polynôme $X^2 - X$ annule f.
- ???

Proposition I.5. Pour $f \in L(E)$, on a $\dim k[f] = \deg \mu_f$.

Proposition I.6. Si f est semblable à g alors $\mu_f = \mu_g$.

Théorème I.7 (Noyaux)**.** Soient $f \in L(E)$ et $P, Q \in k[X]$ tels que $pgcd(P, Q) = 1$ alors $\ker PQ(f) = \ker P(f) \oplus \ker Q(f)$.

Définition I.8. Soit $f \in L(E)$ et $\chi_f(X) = \prod_{i=1}^{r} P_i(X)^\alpha$ sa décomposition en irréductibles. Les sous-espaces caractéristiques de f sont les $(\ker P_i(f))^\alpha$.

Applications I.9. Si $P = \prod (X - a_i)^{\alpha_i}$ et si τ est le shift dans $k^{\mathbb{N}}$, alors $\ker P(\tau).u = \bigoplus (\tau - a_i)^{\alpha_i}$.

II Réduction d'endomorphisme

• II.A Sous-espaces stables et sous-espaces propres

Définition II.1. .
- Soit $f \in L(E)$. Un *sous-espace stable* par f est un sous-espace vectoriel F tel que $f(F) \subset F$.
- Un scalaire λ est *valeur propre* si $\ker(X - \lambda Id) \neq 0$. L'espace $\ker(X - \lambda Id)$ s'appelle le sous-espace propre et un *vecteurs propres* est un élément non nulle de $\ker(X - \lambda Id) \neq= 0$. On appelle sous-espace propre de f associé à λ le noyau de $\lambda(Id - f)$ noté $E_\lambda(f)$.

Exemple II.2. Si f est la matrice avec que des 1 alors f est de rang 1 de valeur propre 0 et n.

Proposition II.3. Si $f(x) = \lambda x$, alors $P(f)(x) = P(\lambda)x$.

Théorème II.4. Les sous-espaces propres de f sont en somme directe.

Proposition II.5. Si u, v commutent alors $\ker u$ et $\operatorname{Im} u$ sont stables par v.

Proposition II.6. Un scalaire λ est valeur propre de f si et seulement si $\det(\lambda - f)$.

Définition II.7. On note $\chi_f(X) = \det(X - f)$ le polynôme caractéristique de f.

Proposition II.8. Si f est semblable à g alors $\chi_f = \chi_g$.

Remarque II.9. f et ${}^t f$ ont même polynôme caractérisque.

Théorème II.10 (Calay-Hamilton)**.** Pour $f \in L(E)$, on a $\chi_f(f) = 0$.

Corollaire II.11. $\mu_f(X) | \chi_f(X)$ et $\deg \mu_f \leq n$.

Applications II.12.
- Calcul de polynôme annulateur.
- ???

• II.B Diagonalisation

Définition II.13. f est dit *diagonalisable* s'il existe une base $(e_1, ..., e_n)$ de vecteurs propres pour f, c'est-à-dire que $Mat_e(f)$ est diagonale.

Remarque II.14. Cette notion est invariante par similitude.

Théorème II.15. Soit $f \in L(E)$. Les propositions suivantes sont équivalentes :
- f est digonalisable.
- Il existe $\lambda_1, \ldots, \lambda_p$ tels que $\ker(u - \lambda_1) + \cdots + \ker(u - \lambda_p) = E$.
- u admet un polynôme annulateur simplement scindé.

Corollaire II.16. Si F est stable par f et $f_{|F}$ est diagonalisable.

Exemple II.17. Les symétries et les projecteurs sont diagonalisables. Les endomorphismes nilpotents non nuls ne sont pas diagonalisables.

Applications II.18.
- Développement [Théorème de Burnside] Un sous-groupe G de $GL_n(\mathbb{C})$ est fini si et seulement si G est d'exposant fini.
- La classe de similitude de M est fermée (resp. bornée) si et seulement si M est diagonalisable (resp : scalaire).

Théorème II.19. Développement [Endomorphismes semi-simples] [A completer]

• II.C Trigonalisation

Définition II.20. f est *trigonalisable*, s'il existe une base e tel que $Mat_e(f)$ soit triangulaire supérieure.

Théorème II.21. Les propositions suivantes sont équivalentes :
- f est trigonalisable.
- f admet un polynôme annulateur scindé.
- χ_f est scindé.

Corollaire II.22. Si k est clos, tout endomorphisme est diagonalisable.

Exemple II.23. Tout endomorphisme nilpotent est trigonalisable.

Applications II.24.
- Soit $M \in Mc_n(\mathbb{R})$ tel que $Spec(M) \subset \{\text{Re} < 0\}$, alors $\exists \lambda > 0, \|exp(tM)\| = O(e^{-\lambda t})$.
- Pour $M \in \mathcal{M}_n(\mathbb{R})$, et $\varepsilon > 0$, il existe une norme N tel que $N(M) \leq \rho(M) + \varepsilon$. On a $\lim_{n\to+\infty} \|M^n\|^(1/n) = \rho(M)$.

Théorème II.25. Soit f_I une famille commutative d'endomorphismes diagonalisables (resp. trigonalisables). Alors il existe une base commune de diagonalisation (resp. trigonalisable).

Théorème II.26 (Théorème de Lie-Kolchin)**.** Développement Si G est un sous-groupe connexe et résoluble de $GL_n(\mathbb{C})$, alors G est conjugué à sous-groupe des matrices triangulaires supérieures inversibles.

III Réductions des endomorphismes auto-dajoints et orthogonaux

• III.A Diagonalisation des endomorphismes auto-adjoints

Ici $k = \mathbb{R}$ ou $\mathbb{C}$.

Théorème III.1. Si f est un endomorphisme auto-adjoint d'un espace euclidien (ou préhilbertien complexe), alors toutes ses valeurs propres complexes sont réelles.

Applications III.2.
- Courant-Fischer : si f est auto-adjoint de valeurs propres $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Alors $\lambda_i = \min_{\dim F = i} \max_{x \in F} \frac{\langle x, f.x\rangle}{||x||^2}$.
- Racine carré : L'application $\begin{array}{ccc} S_n^{++}(\mathbb{R}) & \longrightarrow & S_n^{++}(\mathbb{R}) \\ M & \longmapsto & M^2 \end{array}$ est un C^∞-difféormorphisme.

Applications III.3 (Théorème de l'amitié)**.** Soit G un graphe à n sommets tel que toute paire de sommets admet exactement un sommet adjacent commun. Alors il existe un sommet adjacent à tous les autres.

• III.B Réduction des endomorphismes orthogonaux

Proposition III.4. Si $M \in O_n(\mathbb{R})$, alors toutes ses valeurs propres sont de module 1.

Théorème III.5. Si $M \in O_n(\mathbb{R})$, alors M est orthogonalement semblable à une matrice diagonale par bloc avec blocs I_p, I_q ou R_θ.

Applications III.6.
- Le groupe $SO_n(\mathbb{R})$ est connexe.
- ? ? ?

Théorème III.7. Si $M \in U_n(\mathbb{R})$ alors M est diagonalisable en base orthonormée.

IV Théorèmes de réductions

• IV.A Réduction de Jordan

Théorème IV.1 (Décomposition de Dunford)**.** Soit f tel que χ_f soit scindé. Alors il existe un unique couple (d, n) vérifiant
- d est diagonalisable et n est nilpotent.
- d et n commutent.
- $f = d + n$.

Applications IV.2.
- Calcul de l'exponentiel $exp(f) = exp(d)exp(n)$.
- exp est surjective de $M_n(\mathbb{C})$ dans $GL_n(\mathbb{C})$.
- Toute matrice est semblable à sa transposées.

Théorème IV.3. Développement [Décomposition de Dunford effective] Soit $A \in \mathcal{M}_N(\mathbb{C})$. On note $Q(X) = \prod_{\lambda \in Spec(A)} X - \lambda$. On définit la suite : $A_0 = A$ et $\forall n \in \mathbb{N}, A_{n+1} = A_n - \frac{Q(A_n)}{Q'(A_n)}$. Alors la suite $(A_n)_{n\in\mathbb{N}}$ est bien définie et stationne à la partie diagonale de A.

Théorème IV.4 (Réduction de Jordan)**.** Soit f tel que χ_f est scindé. Alors il existe une base e tel que $Mat_e(f) = diag(J_{\lambda_1}^{r_1}, ..., J_{\lambda_p}^{r_p})$, avec $J_\lambda^r = \lambda I_r + Nil_r$ appelé cellule de Jordan. De plus les matrices $J_{\lambda_1}^r$ son uniques.

Corollaire IV.5. Si k est clos la réduction de Jordan caratérise les classe de similitude de $M_n(k)$.

Applications IV.6.
- Dans $M_n(\mathbb{C})$ toute matrice est semblable à sa transposée et on peut choisir la matrice de passage symétrique : i.e pout tout $f \in L(E)$, il existe une forme bilinéaire symétrique non-dégénérée ϕ telle que f soit autoadjoint pour ϕ.
- Développement [Critère de nilpotence de Cartan] ...

• IV.B Facteurs invariants

Définition IV.7. f est un *endomorphismes cycliques* s'il existe $x \in E$ tel que $(x, f(x), \dots, f^{n-1}(x))$ soit base de E. Un *sous-espace cyclique* est un sous-espace où f agit de façon cyclique.

Définition IV.8. Pour $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ unitaire de degré n. On note $Frob(P)$ la matrice de Frobénius associée à P.

Proposition IV.9. On a équivalence entre :
- f est un endomorphisme cyclique.
- Il existe e base et $P \in k[X]$ tels que $Mat_e(f) = Frob(P)$.
- $\deg P_{min,f} = n$.

Auquel cas $P(X) = \chi_f(X) = P_{min,f}$.

Théorème IV.10 (Invariant de similitudes)**.** Soit f un endomorphisme. Il existe des polynômes unitaires non constants $D_1, \dots, D_r$ et des sous-espaces $E_1, \dots, E_r$ vérifiant :
- $D_1|D_2|\cdots|D_r$.
- f agit de façon cyclique sur E_i et $\chi_{f_{|E_i}} = P_i$.
- $E = E_1 \oplus \cdots \oplus E_r$.

De plus les D_i sont unique et $\mu_f = D_r$, $\chi_f = D_1.D_2...D_r$. Les D_i s'appelle les *facteurs invariants* de f.

Corollaire IV.11. Les facteurs invariants caractérisent les classes de similitude de $L(E)$.

Corollaire IV.12 (Décomposition de Frobénius)**.** Il existe une base e telle que $Mat_e(f) = diag(Frob(D_1), ..., Frob(D_r))$.

Applications IV.13. Soient $K \subset L$ et $M, N \in \mathcal{M}_n(K)$.
- M a le même polynôme minimal sur K et L.
- Si M et N sont semblables sur $\mathcal{M}_n(L)$, alors ils sont semblables sur $\mathcal{M}_n(K)$.

V Développements

- Théorème de l'amitié.
- Décomposition de Dunford effective.
- Théorème de Lie Kolchin.
- Critère de nilpotence de Cartan.
- Endomorphismes semi-simples.
- Théorème de Burnside.
- Théorème Liapouvnov.
- A et B sont semblables si et seulement si $A - XId$ et $B - XId$ sont équivalentes.
- Sur l'exponentielle matricielle.

VI Exercices

Exercice .1 (Gourdon, Alg, Chap.4 Pb. 11)**.** ...

Démonstration. □

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

Références [...]

I Réduction d'endomorphismes

• I.A Sous-espaces stables et sous-espaces propres

Définition I.1. E désigne un espace vectoriel de dimension finie n sur un corps k commutatif.
- Soit $f \in L(E)$. Un *sous-espace stable* par f est un sous-espace vectoriel F tel que $f(F) \subset F$.
- Un scalaire λ est *valeur propre* si $\ker(X - \lambda Id) \neq 0$, et l'espace $\ker(X - \lambda Id)$ s'appelle le sous-espace propre et un *vecteurs propres* est un élément non nulle de $\ker(X - \lambda Id) \neq= 0$. On appelle sous-espace propre de f associé à λ le noyau de $\lambda(Id - f)$ noté $E_\lambda(f)$.

Exemple I.2. Si f est un projecteur non trivial alors $\ker f$ et $\operatorname{Im} f$ sont stables et les valeurs propres de f sont $0, 1$.

Théorème I.3. Les sous-espace propres de f sont supplémentaires.

Proposition I.4 (Caractération matricielle)**.** Soit $(e_i)_{i\in\mathbb{N}}$ une base. Alors $vect(e_1, \dots, e_p)$ est stable par f si et seulement si la matrice de f est de la forme $\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$.

Proposition I.5. Si u, v commutent alors $\ker u$ et $\operatorname{Im} u$ sont stables par v.

Proposition I.6. Si F est stable par f, alors $F^\perp$ est stable par ${}^t f$.

Applications I.7.
- Un hyplerplan stable pour f correspond un vecteur propre pour ${}^t f$ (ex : trigonalisation).
- Si f est un endormorphisme orthogonal ou symétrique d'un espace euclidien, alors ses sous-espaces propres sont orthogonaux.

Proposition I.8. Si tout vecteur est vecteur propre, alors f est une homothétie.

Applications I.9.
- $PGL(E)$ agit de façon fidèle sur $P(E)$.
- Une application linéaire de $\mathbb{R}^2$ qui conserve les angles est une similitude.

• I.B Polynôme caractéristique et sous-espace caractéristiques

Définition I.10. On note $\chi_f(X) = \det(X - f)$ (avec $X - f \in L(E \otimes k(X))$) le polynôme caractéristique de f.

Proposition I.11. Un scalaire λ est valeur propre de f si et seulement si $\det(\lambda - f)$.

Applications I.12. En dimension finie tout endomorphisme admet un vecteur propre (Cf : critère d'hypercylicité de Kitai)

Remarque I.13. f et ${}^t f$ ont même polynôme caractérisque.

Définition I.14. On note μ_f le polynôme minimal de f.

Théorème I.15 (Calay-Hamilton)**.** Pour $f \in L(E)$, on a $\chi_f(f) = 0$.

Corollaire I.16. Le polynôme minimale de f est de degré $\leq n$.

Théorème I.17 (Noyaux)**.** Soient $f \in L(E)$ et $P, Q \in k[X]$ tels que $pgcd(P, Q) = 1$ alors $\ker PQ(f) = \ker P(f) \oplus \ker Q(f)$.

Définition I.18. Soit $f \in L(E)$ et $\chi_f(X) = \prod_{i=1}^r P_i(X)^\alpha$ sa décomposition en irréductibles. Les sous-espaces caractéristiques de f sont les $(\ker P_i(f))^\alpha$.

Applications I.19 (Suite récurrentes linéaires)**.** Soit k de caractéristique 0. Si $P = \prod_{1=1}^r (X - a_i)^{\alpha_i}$ et si τ est le shift dans $k^{\mathbb{N}}$, alors $\ker P(\tau).u = \bigoplus_{i=1}^r \ker(\tau - a_i)^{\alpha_i}$ et $\ker(\tau - a_i)^{\alpha_i} = \left\{(P(n)a_i^n)_{n\in\mathbb{N}} : P \in k[X]_{\alpha-1}\right\}$ si $a_i \neq 0$ et $\ker(\tau - a_i)^{\alpha_i} = \{(x_n)_{n\in\mathbb{N}} : x_0 = x_1 = \cdots = x_{\alpha_i - 1}0\}$ si $a_i = 0$.

II Diagonalisation et trigonalisation

• II.A Diagonalisation

Définition II.1. f est dit *diagonalisable* s'il existe une base $(e_1, \dots, e_n)$ de vecteurs propres pour f, i.e. $Mat_e(f)$ est diagonale.

Remarque II.2. Cette notion est invariante par similitude.

Théorème II.3. Les propositions suivantes sont équivalentes :
- u est digonalisable.
- Il existe $\lambda_1, \dots, \lambda_p$ tels que $\ker(u - \lambda_1) + \cdots + \ker(u - \lambda_p) = E$.
- u admet un polynôme annulateur simplement scindé.

Corollaire II.4. Si F est stable par f et $f_{|F}$ est diagonalisable.

Exemple II.5. Les symétries et les projecteurs sont diagonalisables. Les endomorphismes nilpotents non nuls ne sont pas diagonalisables.

Proposition II.6. Si f est diagonalisable et F un sous-espace stable par f, alors $F = \bigoplus_{\lambda\in Spec(f)} F \cap E_\lambda(f)$.

Applications II.7. ???

Théorème II.8. Développement [Endomorphismes semi-simples] Soit $f \in L(E)$. Alors on a équivalence entre
- Tout sous-espace stable par f admet un supplémentaire stable.
- Le polynôme π_f est sans facteurs carrés.

• II.B Trigonalisation

Définition II.9. f est *trigonalisable* s'il existe une base e tel que $Mat_e(f)$ soit triangulaire supérieure.

Théorème II.10. Les propositions suivantes sont équivalentes :
- f est trigonalisable.
- f admet un polynôme annulateur scindé.
- χ_f est scindé.

Corollaire II.11. Si k est clos, tout endomorphisme est diagonalisable.

Exemple II.12. Tout endomorphisme nilpotent est trigonalisable.

Proposition II.13. Si $M = [m_{ij}]_{i,j} \in \mathcal{M}_n(k)$ est triangulaire supérieur, alors son polynôme caractéristique est $\prod_{i=1}^{n} X - m_{ii}$ et ses valeurs propres sont les coefficients diagonaux m_{ii}.

• II.C Diagonalisation et trigonalisation simultanées

Théorème II.14. Soit f_I une famille commutative d'endomorphismes diagonalisables (resp. trigonalisable). Alors il existe une base commune de diagonalisation (resp. trigonalisable).

Applications II.15.
- Les représentations irréductibles d'un groupe abélien fini sont de dimension 1.
- ? ? ?

Théorème II.16 (Théorème de Lie-Kolchin)**.** Développement Si G est un sous-groupe connexe et résoluble de $GL_n(\mathbb{C})$, alors G est conjugué à sous-groupe des matrices triangulaires supérieures inversibles.

III Théorèmes de réductions

• III.A Décomposition de Dunford

Théorème III.1 (Décomposition de Dunford)**.** Soit f tel que χ_f soit scindé. Alors il existe un unique couple (d, n) vérifiant
- d est diagonalisable et n est nilpotent.
- d et n commutent.
- $f = d + n$.

Applications III.2.
- Calcul de l'exponentiel $exp(f) = exp(d)exp(n)$.
- exp est surjective de $M_n(\mathbb{C})$ dans $GL_n(\mathbb{C})$.

• III.B Réduction de Jordan

Remarque III.3. Un sous-espace stable correspond à un sous-$k[X]$-module

Théorème III.4 (Réduction de Jordan)**.** Soit f tel que χ_f est scindé. Alors il existe une base e tel que $Mat_e(f) = diag(J^{r_1}_{\lambda_1}, \dots, J^{r_p}_{\lambda_p})$, avec $J^r_\lambda = \lambda I_r + Nil_r$ appelé cellule de Jordan. De plus les matrices $J^r_{\lambda_1}$ son uniques.

Corollaire III.5. Si k est clos la réduction de Jordan caratérise les classe de similitue de $M_n(k)$.

Applications III.6.
- Dans $M_n(\mathbb{C})$ toute matrice est semblable à sa transposée et on peut choisir la matrice de passage symétrique : i.e pout tout $f \in L(E)$, il existe une forme bilinéaire symétrique non-dégénérée ϕ telle que f soit autoadjoint pour ϕ.
- Développement [Critère de nilpotence de Cartan] ...

IV Endomorphismes cycliques et facteurs invariants

• IV.A Sous-espaces cycliques

Définition IV.1. Soit $f \in L(E)$
- Un *sous-espace cyclique* est un sous-espace du type $K[f].x$.
- f est dit cyclique s'il existe $x \in E$ tel que $K[f].x = E$.

Si le vecteur x engendre l'espace, alors $(x, f(x), \dots, f^{n-1}(x))$ est une base et la matrice de f est $Frob(P)$.

Théorème IV.2. Soit $f \in L(E)$. Les propositions suivantes sont équivalentes
- f est une endomorphisme cyclique.
- Il existe $x \in E$ tel que $(x, f(x), \dots, f(x)^{n-1})$ soit une base.
- $\deg \mu_f(X) = n$.

Proposition IV.3. Si f est un endomorphisme cyclique, alors on a une bijection entre $\begin{array}{ccc} \{\text{diviseurs de } \mu_f\} & \longrightarrow & \{\text{sous-espaces stables}\} \\ P(X) & \longmapsto & \ker P(f) \end{array}$, et pareil avec $ImP(f)$.

• IV.B Facteurs invariants

Définition IV.4. Pour $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ unitaire de degré n. On note $Frob(P)$ la matrice de Frobénius associé à P.

Théorème IV.5 (Invariant de similitudes)**.** Soit f un endomorphisme. Il existe des polynômes unitaires non constants $D_1, \dots, D_r$ et des sous-espaces $E_1, \dots, E_r$ vérifiant :
- $D_1 | D_2 | \cdots | D_r$.
- f agit de façon cyclique sur E_i et $\chi_{f_{|E_i}} = P_i$.
- $E = E_1 \oplus \cdots \oplus E_r$.

De plus les D_i sont unique et $\mu_f = D_r$, $\chi_f = D_1.D_2...D_r$. Les D_i s'appelle les *facteurs invariants* de f.

Corollaire IV.6. Les facteurs invariants caractérisent les classes de similitude de $L(E)$.

Corollaire IV.7 (Décomposition de Frobénius)**.** Il existe une base e telle que $Mat_e(f) = diag(Frob(D_1), ..., Frob(D_r))$.

Applications IV.8. Soient $K \subset L$ et $M, N \in \mathcal{M}_n(K)$.

- M a le même polynôme minimal sur K et L.
- Si M et N sont semblables sur $\mathcal{M}_n(L)$, alors ils sont semblables sur $\mathcal{M}_n(K)$.

V Développements

- Théorème de Lie-Kolchin.
- Endomorphismes semi-simples.
- Théorème Molien.

VI Exercices

126 - Endomorphismes diagonalisables en dimension finie

Références [Arnaudies 1], [Escofier (alg. licence)].

I Valeurs propres et sous-espaces propres

• I.A Définitions

Soit k un corps, E un k-espace vectoriel de dimension finie et $A \in L(E)$.

Définition I.1. Une *valeur propre* de A est un scalaire $\lambda \in k$ tel que : $\exists x \neq 0, A\lambda = \lambda.x$. Le vecteur x est alors *vecteur propre* de A pour la valeur propre λ. Le *sous-espace propre* associé à $\ker(A - \lambda)$.

Exemple I.2. Projecteurs. Symétries.

Proposition I.3. Les sous-espaces propres sont en somme directe. En particulier il y a au plus $\dim E$ valeurs propres.

Proposition I.4. Si A et B commutent, alors les sous-espace propres de l'un sont stables par l'autre.

Définition I.5. On appelle *spectre* de A, l'ensemble des ses valeurs propres dans une clôture algébrique.

• I.B Polynômes d'endomorphismes et sous-espace stables

Si $A \in L(E)$, alors on a un morphisme de k-algèbre $k[X] \to L(E), P(X) \mapsto P(A)$.

Définition I.6. Le polynôme minimal de A est le générateur unitaire du noyau de ce morphisme.

Théorème I.7 (Noyaux)**.** Soient $f \in L(E)$ et $P, Q \in k[X]$ tels que $pgcd(P, Q) = 1$ alors $\ker PQ(f) = \ker P(f) \oplus \ker Q(f)$.

Définition I.8. Soit $f \in L(E)$ et $\chi_f(X) = \prod_{i=1}^{r} P_i(X)^{\alpha}$ sa décomposition en irréductibles. Les sous-espaces caractéristiques de f sont les $(\ker P_i(f))^{\alpha}$.

Applications I.9. Si $P = \prod(X - a_i)^{\alpha_i}$ et si τ est le shift dans $k^{\mathbb{N}}$, alors $\ker P(\tau).u = \bigoplus(\tau - a_i)^{\alpha_i}$.

Théorème I.10. Un scalaire $\lambda \in k$ est valeur propre de A si et seulement si $\det(\lambda - A) = 0$.

Définition I.11. Le *polynôme caractéristique* de A est $\chi_A(X) = \det(X - A)$.

Proposition I.12.
- A non injective $\iff 0$ est valeur propre de A et $\chi_A(0) = 0$.
- A non injective $\iff \exists \lambda \in Spec(A), P(\lambda) = 0$.

Théorème I.13 (Calay-Hamilton)**.** Pour $f \in L(E)$, on a $\chi_f(f) = 0$.

Corollaire I.14. $\mu_f(X) | \chi_f(X)$ et $\deg \mu_f \leq n$.

Applications I.15.
- Calcul de polynôme annulateur.
- ? ? ?

Proposition I.16. La dimension du sous-espace propre $\ker(A - \lambda)$ est inférieur à la multiplicité de λ dans $\chi_A(X)$.

II Diagonalisation

• II.A Définition

Définition II.1. Un endomorphisme est diagonalisable, s'il existe une base de vecteurs propres. Auquel cas sa matrice dans cette base est diagonale.

Exemple II.2.
- Les projecteurs et symétries.
- ? ? ?

Proposition II.3. A est diagonalisable si et seulement si A admet un polynôme annulateur simplement scindé.

Corollaire II.4. Si A est diagonalisable et si F est stable par A, alors $A_{|F}$ est diagonalisable. On a même $F = \bigoplus \ker(A - \lambda) \cap F$.

Définition II.5. Si k est clos et si $\chi_A(X) = \prod(X - \lambda_i)^{\alpha_i}$, les sous-espaces caractériques de A sont les $\ker(A - \lambda_i)^(\alpha_i)$

Proposition II.6. Les projecteurs sur les sous-espace caractéristiques sont polynômiaux en A.

Proposition II.7 (Diagonalisation simultanée)**.** Si $(A_i)_{i \in I}$ commutent et sont diagonalisables, alors les $(A_i)_{i \in I}$ sont codiagonalisables.

Applications II.8. Sous-groupes commutatifs de $GL_n(\mathbb{C})$.

• II.B Décomposition de Dunford

Théorème II.9 (Dunford)**.** Si $\chi_A(X)$ est scindé, alors il existe un unique endomorphisme diagonalisable D et un nilpotent N tels que $A = D + N$ et $DN = ND$.

L'hypothèse est vérifiée si k est clos.

Théorème II.10. Développement [Décomposition de Dunford effective] Soit $A \in \mathcal{M}_N(\mathbb{C})$. On note $Q(X) = \prod_{\lambda \in Spec(A)} X - \lambda$. On définit la suite : $A_0 = A$ et $\forall n \in \mathbb{N}, A_{n+1} = A_n - \dfrac{Q(A_n)}{Q'(A_n)}$. Alors la suite $(A_n)_{n \in \mathbb{N}}$ est bien définie et stationne à la partie diagonale de A.

Applications II.11. On a $Spec(A \otimes B) = Spec(A).Spec(B)$.

Théorème II.12 (Réduction de Jordan)**.** Soit f tel que χ_f est scindé. Alors il existe une base e tel que $Mat_e(f) = diag(J_{\lambda_1}^{r_1}, ..., J_{\lambda_p}^{r_p})$, avec $J_\lambda^r = \lambda I_r + Nil_r$ appelé cellule de Jordan. De plus les matrices $J_{\lambda_1}^r$ son uniques.

Théorème II.13 (Réduction de Jordan)**.** Soit f tel que χ_f est scindé. Alors il existe une base e tel que $Mat_e(f) = diag(J_{\lambda_1}^{r_1}, ..., J_{\lambda_p}^{r_p})$, avec $J_\lambda^r = \lambda I_r + Nil_r$ appelé cellule de Jordan. De plus les matrices $J_{\lambda_1}^r$ son uniques.

Applications II.14.
- Dans $M_n(\mathbb{C})$ toute matrice est semblable à sa transposée et on peut choisir la matrice de passage symétrique : i.e pout tout $f \in L(E)$, il existe une forme bilinéaire symétrique non-dégénérée ϕ telle que f soit autoadjoint pour ϕ.
- Développement [Critère de nilpotence de Cartan] ...

• II.C Endomorphismes semi-simples

Définition II.15. Un endomorphisme A est semi-simple si tout sous-espace stable admet un supplémentaire stable.

Proposition II.16. Un endomorphisme A est semi-simple si et seulement si $\mu_A(X)$ est sans facteurs carrés.

En particulier si k est parfait, alors celà équivaut à A diagonalisable dans une clôture algébrique.

III Diagonalisation dans $\mathbb{R}$ et $\mathbb{C}$

• III.A Propriétés topologiques

Définition III.1. Un endomorphisme f est trigonalisable s'il exsite une base e telle que $Mat_e(f)$ soit triangulaire supérieure.

Théorème III.2.
- Sur $\mathbb{C}$, l'ensemble des matrices diagonalisables est dense.
- Sur $\mathbb{R}$ L'ensemble des matrices diagonalisables a pour adhérence l'ensemble des matrices trigonalisable.

Applications III.3. Théorème de Calay-Hamilton : $\chi_A(A) = 0$.

• III.B Réductions des endomorphismes auto-dajoints et orthogonaux

Ici $k = \mathbb{R}$ ou $\mathbb{C}$.

Théorème III.4. Si f est un endomorphisme auto-adjoint d'un espace euclidien (ou préhilbertien complexe), alors toutes ses valeurs propres complexes sont réelles.

Applications III.5.
- Courant-Fischer : si f est auto-adjoint de valeurs propres $\lambda_1 \leq \lambda_2 \leq ... \leq \lambda_n$. Alors $\lambda_i = \min_{\dim F = i} \max_{x \in F} \frac{\langle x, f.x \rangle}{||x||^2}$.
- Racine carré : L'application $\begin{array}{ccc} S^{++}(\mathbb{R}) & \longrightarrow & S^{++}(\mathbb{R}) \\ M & \longmapsto & M^2 \end{array}$ est un C^∞-difféormorphisme.

Applications III.6 (Théorème de l'amitié)**.** Soit G un graphe à n sommets tel que toute paire de sommets admet exactement un sommet adjacent commun. Alors il existe un sommet adjacent à tous les autres.

IV Développements

- Théorème de l'amitié.
- Décomposition de Dunford effective.
- Endomorphismes semi-simples.

V Exercices

127 - Exponentielle de matrices. Applications

Références [MT86], [Gou94], [Rombaldi ?]

I Généralités sur l'exponentielle matricielle

• I.A Définition

Définition I.1. Sur $\mathcal{M}_n(\mathbb{R})$ ou $\mathcal{M}_n(\mathbb{C})$, la série $\sum_{n=0}^{+\infty} \frac{A^n}{n!}$ converge normalement sur tout compact pour n'importe quelle norme subordonnée. On note exp sa somme.

Exemple I.2.
- $exp\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix} = \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}$.
- $exp(diag(\lambda_1, \dots, \lambda_n)) = diag(e^{\lambda_1}, \dots, e^{\lambda_n})$.
- Si N est nilpotent, alors $exp(N) = I_n + N + \frac{N^2}{2} + \dots + \frac{N^{n-1}}{(n-1)!}$.

Proposition I.3. On note $k = \mathbb{R}$ ou $\mathbb{C}$. Soient $A, B \in \mathcal{M}_n(k)$.
- Si A et B commutent, alors $exp(A+B) = exp(A)exp(B)$.
- $exp(-A) = exp(A)^{-1}$.
- Pour $P \in GL_n(\mathbb{K})$, $Pexp(A)P^{-1} = exp(PAP^{-1})$.
- $exp({}^tA) = {}^t exp(A)$. Donc $exp(S_n(\mathbb{R})) \subset S_n(\mathbb{R})$.
- $\det exp(A) = e^{Tr(A)}$.

Proposition I.4. $exp(A)$ est polynômial en A.

• I.B Inversion de l'exponentiel

Définition I.5. Pour $X \in B(0,1)$, on note $\log(1+X) = \sum_{k=1}^{\infty} (-1)^{k-1} \frac{X^k}{k}$.

Proposition I.6.
- L'exponentiel réalise une bijection des matrices nilpotentes vers les matrices unitpotents, et sa bijection réciproque est le logarithme.
- Pour tout $M \in B(I_n, 0)$, on a $exp(\log M) = M$.

Proposition I.7.
- Si $A = D + N$ est la décomposition de Dunford de A, alors $exp(A) = exp(D) + exp(D)(exp(N) - I_n)$ est la décomposition de Dunford de $exp(A)$.
- Si $X \in \mathcal{M}_n(\mathbb{C})$ est diagonalisable si et seulement si $exp(\mathbb{C})$ est diagonalisable.
- On a $exp(\mathcal{M}_n(\mathbb{C})) = GL_n(\mathbb{C})$ et $exp(\mathcal{M}_n(\mathbb{R})) = GL_n(\mathbb{R})^2$. Toute matrice complexe inversible admet une racine $p$em.

Exemple I.8. $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ ne sont pas dans $exp(\mathcal{M}_n(\mathbb{R}))$.

II Régularité

Définition II.1. Pour $A, B \in \mathcal{M}_n(\mathbb{C})$, on note $\begin{array}{rccc} A \otimes B : & \mathcal{M}_n(\mathbb{C}) & \longrightarrow & \mathcal{M}_n(\mathbb{C}) \\ & X & \longmapsto & AXB \end{array}$.

Théorème II.2. Développement [Différentielle] La fonction exp est C^∞. De plus
- $Dexp(X) = exp(X \otimes I_n) F(X \otimes I_n - I_n \otimes X)$, avec $F(T) = T^{-1}(1 - e^{-T})$.
- X est point critique de exp si et seulement si $\exists \lambda, \mu \in Spec(X), \lambda - \mu \in 2i\pi\mathbb{Z}^*$.

Théorème II.3.
- L'application $\begin{array}{ccc} S_n & \longrightarrow & S_n^{++}(\mathbb{R}) \\ S & \longmapsto & exp(S) \end{array}$ est un C^∞-difféomorphisme.
- Décomposition polaire : si G est un sous-groupe de $GL_n(\mathbb{R})$ stable par adjonction tel que $G \cap S_n^{++}(\mathbb{R})$ est stable par racine carré, alors l'application $\begin{array}{ccc} (G \cap S_n^{++}(\mathbb{R})) \times (G \cap O_n(\mathbb{R})) & \longrightarrow & G \\ (S, O) & \longmapsto & SO \end{array}$ est un C^∞-difféomorphisme.

Applications II.4.
- Le groupe $O(p,q)$ a 4 composantes connexes si $p, q \geq 1$.
- ? ? ?

• II.A Sous-groupes de $Gl_n(\mathbb{R})$

Définition II.5. Un sous-groupe à un paramètre est l'image d'un morphisme de groupe de $\mathbb{R}$ vers $GL_n(\mathbb{R})$.

Théorème II.6. Tout sous-groupe à un paramètre est du type $exp(tA)$ (en particulier est C^∞).

Définition II.7. Soit G un sous-groupe fermé de $GL_n(\mathbb{R})$. Son algèbre de Lie est : $L_G = \left\{ X \in \mathcal{M}_n(\mathbb{R}) \mid \forall t \in \mathbb{R}, exp(tX) \in G \right\}$.

Proposition II.8. L'espace L_G est un sous-espace vectoriel stable par crochet de Lie.

Théorème II.9 (Cartan). Développement Tout sous-groupe fermé de $GL_n(\mathbb{R})$ est une variété lisse.

Exemple II.10.
- $L_{GL_n(\mathbb{R})} = \mathcal{M}_n(\mathbb{R})$, $L_{SL_n(\mathbb{R})} = \ker Tr$.
- $L_{O_n(\mathbb{R})} = L_{SO_n(\mathbb{R})} = Antsym_n(\mathbb{R})$.
- $SP_{2n}(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) : {}^tMJM = J\}$, $L_{SP_{2n}(\mathbb{R})} = \{X \in \mathcal{M}_n(\mathbb{R}) : {}^tXJ + JX = 0\}$.

Proposition II.11. Il existe un voisinage U de $I_n \in GL_n(\mathbb{C})$ tel que $\{I_n\}$ est le seul sous-groupe de $GL_n(\mathbb{R})$ inclus dans U.

III Applications aux équations différentielles

• III.A Résolution d'équations linaires à coefficients constants

Proposition III.1. Si $X(t)$ et $X'(t)$ commutent, alors $\frac{d}{dt}exp(X(t)) = X'(t)exp(X(t))$.

Théorème III.2.
- La résolvante de l'équation $X'(t) = AX(t)$ est $exp(tA)$.
- La solution de l'EDL $X'(t) = AX(t)$, $X(0) = X_0$ est $X(t) = exp(tA).X_0$.

Remarque III.3. En pratique on réduit A pour calculer $exp(tA)$.

Exemple III.4. Si A est une matrice antisymétrique de $\mathbb{R}^3$, donc la matrice du produit vectoriel par un vecteur u, alors les orbites sont des cercles dont l'axe est u.

• III.B Théorème de Liapounov

Définition III.5. Une matrice $A \in \mathcal{M}_n(\mathbb{R})$ est dite stable si $Spec(A) \subset \{\mathrm{Re} < 0\}$.

Proposition III.6. Pour $A \in \mathcal{M}_n(\mathbb{C})$, on a : $\lim_{t\to+\infty} exp(tA) = 0 \iff A$ est stable.

Théorème III.7. Développement [Liapounov] Soit E un $\mathbb{R}$-espace vectoriel normé, $f : E \to E$ un champ de vecteurs tel que $f(0) = 0$ et $Df(0)$ stable. On note Φ son flot. Alors il existe un voisinage U de 0 et $\lambda > 0$ tel que

$$\forall x \in U, \|\phi_t(x)\| \leq e^{-t\lambda}.$$

.

Exemple III.8. ? ? ?

IV Développements

- Points critiques de l'exponentiel.
- Théorème de Cartan.
- Théorème de stabilité de Liapounov.
- Image de l'exponentiel.

V Exercices

128 - Endomorphismes trigonalisables. Endomorphismes nilpotents

Références [Arnaudies 1 ?]

I Trigonalisation

• I.A Sous-espaces stables et drapeaux

Soit E un espace vectoriel de dimension fini sur un corps k et $A \in L(E)$.

Définition I.1.
- Un sous-espace F est *stable* par A si $A(F) \subset F$.
- Un scalaire $\lambda \in k$ est *valeur propre* si $\ker(A-\lambda) \neq \{0\}$ et tout vecteur de $\ker(A-\lambda) - \{0\}$ est dit *vecteur propre*.

Exemple I.2.
- Le noyau, l'image et les sous-espaces propres de A sont stables par A.
- ? ? ?

Proposition I.3 (Caractération matricielle)**.** Soit $(e_i)_{i\in\mathbb{N}}$ une base. Alors $vect(e_1,\dots,e_p)$ est stable par f si et seulement si la matrice de f est de la forme $\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$.

Proposition I.4. Si u, v commutent alors $\ker u$ et $\operatorname{Im} u$ sont stables par v.

Proposition I.5. Si F est stable par f, alors $F^\perp$ est stable par ${}^t f$.

Applications I.6. Un hyplerplan stable pour f correspond un vecteur propre pour f^*.

Définition I.7. Un *drapeau* est une suite de sous-espaces croissants $F_0 \subset F_1 \subset \cdots\cdots F_n$ tel que $\dim F_k = k$ pour tout $k \in [1,n]$.

Proposition I.8. Si $(E_i)_{i\in[0,n]}$ est un drapeau, alors il existe une base adapté telle que $\forall i \in [0,n], Vect(e_0,\dots,e_i) = E_i$.

• I.B Endomorphismes trigonalisables

Définition I.9. A est trigonalisable A stabilise un drapeau. Auquel cas sa matrice dans une base adapté au drapeau est triangulaire supérieure.

Proposition I.10. Si $M = [m_{ij}]_{i,j} \in \mathcal{M}_n(k)$ est triangulaire supérieur, alors son polynôme caractéristique est $\prod X - m_{ii}$ et ses valeurs propres sont les coefficients diagonaux m_{ii}.

Théorème I.11. Les propositions suivantes sont équivalentes :
- f est trigonalisable.
- f admet un polynôme annulateur scindé.
- χ_f est scindé.

Corollaire I.12. Si k est clos, tout endomorphisme est diagonalisable.

Théorème I.13 (Trigonalisation simultanée)**.** Si $(A_i)_{i\in I}$ est une famille commutative d'endomorphismes trigonalisables, alors elle est cotrigonalisable.

Théorème I.14 (Théorème de Lie-Kolchin)**.** Développement Si G est un sous-groupe connexe et résoluble de $GL_n(\mathbb{C})$, alors G est conjugué à sous-groupe des matrices triangulaires supérieures inversibles.

II Endomorphismes nilpotents

• II.A Définition et propriétés

Définition II.1. Soit $A \in L(E)$. On dit que A est *nilpotent* si il existe $N \in \mathbb{N}$ tel que $A^N = 0$. Le plus petit N est l'*indice de nilpotence*.

Proposition II.2. Toute matrice nilpotente est trigonalisable.

Proposition II.3. Soit $A \in L(E)$ nilpotent. On note $K_i = \ker A^i$ pour $i \in [1,n]$. Alors la suite $(K_i)_{i\in[1,n]}$ croît strictement puis stationne à E.

Corollaire II.4.
- L'indice de nilpotence est inférieure à $\dim E$.
- Pour $A \in L(E)$ et $n = \dim E$: A est nilpotent $\iff A^n = 0 \iff \chi_A(X) = X^n \iff Spec(A) = \{0\}$.

Applications II.5. ? ? ?

Définition II.6. Si $F(X) = \sum_{i=0}^{+\infty} a_i X^i \in k[[X]]$ et A un nilpotent, alors on pose $F(A) = \sum_{i=0}^{n-1} a_i A^i$.

Proposition II.7.
- Si A est nilpotent alors $Id - A$ est inversible d'inverse $\sum_{i=0}^{n-1} A^i$.
- Pour A nilpotent, on a $exp(Ln(1+A)) = 1 + A$.

Applications II.8.
- Pour $P(X) \in \mathbb{R}[X]$, la fonction (ou série formelle) $e^{\lambda X}P(X)$ a pour primitive $e^{\lambda X}(\lambda^{-1} - \lambda^{-2}P'(X) + \lambda^{-3}P^{(2)}(X) - \cdots)$.
- ? ? ?

Proposition II.9. Si $\forall k \in [1,n], Tr(A^k) = 0$, alors A est nilpotent.

Applications II.10. Développement [Théorème de Burnside] Tout sous-groupes de $GL_n(\mathbb{R})$ d'exposant fini est fini.

III Décomposition de Dunford

Théorème III.1 (Décomposition de Dunford)**.** Soit f tel que χ_f soit scindé. Alors il existe un unique couple (d, n) vérifiant
- d est diagonalisable et n est nilpotent.
- d et n commutent.
- $f = d + n$.

Théorème III.2. Développement [Décomposition de Dunford effective] Soit $A \in \mathcal{M}_N(\mathbb{C})$. On note $Q(X) = \prod_{\lambda \in Spec(A)} X - \lambda$. On définit la suite : $A_0 = A$ et $\forall n \in \mathbb{N}, A_{n+1} = A_n - Q'(A_n)^{-1}Q(A_n)$. Alors la suite $(A_n)_{n\in\mathbb{N}}$ est bien définie et stationne à la partie diagonale de A.

Théorème III.3. Développement [Critère de Nilpotence] Soient k un corps clos de caractéristique nulle et E un k-espace vectoriel de dimension finie et $G \subset F$ deux sous-espaces vectoriels de $L(E)$. On note T le sous-ensemble de $GL(E)$ défini par

$$T = \Big\{ M \in L(E) : \forall f \in F, [M, f] \subset G \Big\}.$$

Soit $M \in T$ tel que $\forall N \in T, Tr(MN) = 0$. Alors M est nilpotent.

• III.A Classification

Soit $A \in L(E)$ nilpotent.

Proposition III.4.
- La suite $(\ker A^i)_{i\in[0,n]}$ est croissante strictement puis stationne (cf plus haut).
- La suite $(\dim\ker A^{i+1} - \dim\ker A^{i+1})_{i\in[0,n]}$ est décroissante.

Définition III.5. Soit A nilpotent. Pour $i \in [1, n]$, on note $a_i = \dim(\ker A^i / \ker A^{i-1}$. On appelle $(a_1, \ldots, a_n)$ le tableau de Young de A

Proposition III.6.
- Pour $i \in [1, n]$, on a $\dim\ker A^i = a_1 + \cdots + a_i$.
- La suite $(a_i)_{i\in[1,n]}$ forment une partition de n.

Théorème III.7 (Réduction des matrices nilpotentes)**.** [A completer]

Applications III.8 (Réduction de Jordan)**.** Soit f tel que χ_f est scindé. Alors il existe une base e tel que $Mat_e(f) = diag(J^{r_1}_{\lambda_1}, ..., J^{r_p}_{\lambda_p})$, avec $J^r_\lambda = \lambda I_r + Nil_r$ appelé cellule de Jordan. De plus les matrices $J^r_{\lambda_1}$ son uniques.

IV Développements

- Critère de Nilpotence.
- Théorème de Lie Kolchin.
- Décomposition de Dunford effective.
- Théorème de Burnside.
- Théorème d'Engel.

129 - Algèbre des polynômes d'un endomorphisme en dimension finie. Applications

Références [...]

Introduction [A compléter]

I Algèbre $K[u]$

• I.A Définitions

On note K un corps et E, K-espace vectoriel de dimension finie et $u \in L(E)$.

Définition I.1. Si $P(X) = \sum_{i=0}^{d} a_i X^i$, alors on pose $P(u) = \sum_{i=0}^{d} a_i X^i$.

L'application $P(X) \mapsto P(u)$ est un morphisme d'algèbre et on note $K[u]$ son image.

Définition I.2. L'ensemble $\Big\{P(X) \in K[X] \mid P(u) = 0\Big\}$ est un idéal non nul et on note $\mu_u(X)$ son générqteur unitaire.

Exemple I.3. Si u est nilpotent, alors $\mu_u(X) = X^k$ avec k l'indice de nilpotence,

• I.B Propriétés de $K[u]$

Proposition I.4.
- L'algèbre $K[u]$ est isomorphe à $K[X]/(\mu_u)$.
- Pour $Q(X) \in K[X]$ et $R(X) = Q(X) \mod \mu_u(X)$, on a $Q(u) = R(u)$.
- Pour $Q(X) \in K[X]$, l'endomrophisme $Q(u)$ est inversible si et seulement si $pgcd(Q, \mu_u) = 1$.

Corollaire I.5. $\dim K[u] = \deg \mu_u$.

Proposition I.6. On note $C(u)$ le commutant de u. Alors $K[u] \subset C(u)$ et $C(u) = K[u]$ si et seulement si u est cyclique (cf plus bas).

Applications I.7. ? ? ?

II Réduction

• II.A Critère de réduction

Définition II.1. Le polynôme caractéristique de u est $\det(X - u)$.

Théorème II.2 (Noyau)**.** Si $pgcd(P, Q) = 1$, alors $\ker PQ(u) = \ker P(u) \oplus \ker Q(u)$.

Applications II.3. Si $P = \prod (X - a_i)^{\alpha_i}$ et si τ est le shift dans $k^{\mathbb{N}}$, alors

$$\ker P(\tau).u = \bigoplus (\tau - a_i)^{\alpha_i}.$$

Proposition II.4. u est diagonalisable (resp. trigonalisable) si et seulement si u admet un polynôme annulateur simplement scindé (resp. scindé).

Applications II.5.
- Si u est diagnalisable et si F est stable, alors $u_{|F}$ est diagonalisable.
- Si K est clos, alors tout endomorphisme est trigonalisable.

Théorème II.6 (Dunford)**.** Si $\chi_A(X)$ est scindé, alors il existe un unique couple $(d, n) \in L(E)^2$ tel que $u = d + n$, d diagonalisable, n nilpotent et $dn = nd$.

De plus d et n sont polynômiales en u.

Applications II.7.
- L'exponentiel de $\mathcal{M}_n(\mathbb{C}) \to GL_n(\mathbb{C})$ est surjective.
- ? ? ?

Développement Méthode effective de décomposition de Dunford.

• II.B Structure de $K[X]$-module sur E et réduction de Frobénius

Soit $u \in L(E)$. Pour $x \in E$, on note $P.x = P(u).x$. Celà munie alors E d'une structure de $K[u]$-module. On note $\mu_x(X)$ le générateur de $\Big\{P \in K[X] \mid P.x = 0\Big\}$. Et on note $E_x = \{P.x \mid P \in K[X]\}$ ($\cong K[X]/(\mu_x)$ en tant qu'espace vectoriel).

Définition II.8. On dit que u est cyclique s'il existe $x \in E$ tel que $E_x = E$. Auquel cas $(x, u.x, \dots, u^{n-1}.x)$ est une base et la matrice de u est la matrice de frobenius $Frob(\mu_u)$.

Théorème II.9. Développement [Réduction de Frobénius] ...

Applications II.10. Soient $K \subset L$ et $M, N \in \mathcal{M}_n(K)$.
- M a le même polynôme minimal sur K et L.
- Si M et N sont semblables sur $\mathcal{M}_n(L)$, alors ils sont semblables sur $\mathcal{M}_n(K)$..

• II.C Endomorphismes semi-simples

[A completer]

III Séries entières d'endomorphismes dans $\mathbb{R}$ et $\mathbb{C}$

• III.A Généralité

Proposition III.1. Si $F(T)$ a pour rayon de convergence R, alors pour $X \in M_n(\mathbb{C})$ de rayon spectral $< R$, la série $\sum_{n \in \mathbb{N}} a_n X^n$ converge. On note $F(X)$ sa somme.

En particulier $F(A)$ existe si A est nilpotent ou si $R = +\infty$.

• III.B Exponentiel

Théorème III.2. Développement [Points critiques de l'exponentielle] On note $F(T) = T^{-1}(1 - e^{-T})$. Pour $X \in M_n(\mathbb{C})$,

$$Dexp(X) = e^X.F(ad_X),$$

où $ad_X \in L(M_n(\mathbb{C}))$ et $ad_X.M = XM - MX$.

$$Dexp(X) \text{ non inversible} \Leftrightarrow \exists \lambda, \mu \in Spec(X), \lambda - \mu \in 2i\pi\mathbb{Z}^*.$$

Applications III.3. L'application $U_n(\mathbb{C}) \times H_n(\mathbb{C}) \to GL_n(\mathbb{C})$ est un $\mathbb{C}^\infty$-difféomorphisme.

IV Développements

- Exponentielle matricielle.
- Théorème de Burnside.
- Sous-espace stable d'un endomorphisme cyclique.
- Théorème de Gershorin.
- Décomposition de Dunford effective.

V Exercices

Exercice .1 (Gourdon, Alg, Chap.4 Pb. 11)**.** Soient $A, B \in \mathcal{M}_n(\mathbb{C})$. Montrer que A et B ont une valeur propre commune si et seulement si

$$\exists P \in \mathcal{M}_n(\mathbb{C}) \setminus \{0\}, AP = PB.$$

Démonstration. Si A et B on une valeur propre commune λ, alors on prend $e \in \mathbb{C}^n$ tel que $Ae = \lambda e$ et $\phi \in \mathbb{C}^{n*}$ tel que $\phi.B = \lambda\phi$. On prend alors $P = e.\phi$.

Récriproquement, supposons que A et B n'aient pas de valeur propres communes, et soit $P \in \mathcal{M}_n(\mathbb{C})$ tel que $AP = PB$. Par récurrence sur $k \in \mathbb{N}$, on a $A^kP = PB^k$, donc

$$\forall F(X) \in \mathbb{C}[X], F(A)P = PF(B).$$

En prenant $F(X) = \chi_a(X)$, on a $P\chi_A(B) = 0$. Or les valeurs propres de A et B sont disjoints, donc $\chi_A(B)$ est inversible et $P = 0$. □

Exercice .2 (Gourdon, Alg, Chap.4 Pb. 14)**.** On note $(f_{n-1}, \dots, f_0)$ les polynômes de $\mathbb{Z}[(X_{i,j})_{i,j}]$ tels que

$$\forall A \in \mathcal{M}_n(k), \chi_A(X) = X^n + f_{n-1}(A)X^{n-1} + \cdots + f_0(A).$$

Soit $g \in k[(X_{i,j})_{i,j}]$ tel que

$$\forall A, B \in \mathcal{M}_n(k), g(AB) = g(BA).$$

Montrer que g est polynômial en les $(f_i)_{i\in[0,n-1]}$.

Démonstration. On remarque que g est invariant par conjugaison. La fonction

$$\begin{array}{ccc} \mathbb{C}^n & \longrightarrow & \mathbb{C} \\ (\lambda_1, \dots, \lambda_n) & \longmapsto & g(diag(\lambda_1, \dots, \lambda_n)) \end{array},$$

est invariante par permutation, donc est du type $P(\sigma_1, \dots, \sigma_n)$. Les fonctions g et $P(f_1, \dots, f_n)$ coïncident sur l'ensembles des matrices diagonalisable, donc sont égales. □

130 - Matrices symétriques réelles, matrices hermitiennes

Références [? ? ?]

I Matrices symétriques et formes bilinéaires

• I.A Transposition et conjugaison

On se place dans $\mathcal{M}_n(\mathbb{R})$ ou $\mathcal{M}_n(\mathbb{C})$.

Définition I.1. – Si $M = [m_{i,j}] \in \mathcal{M}_n(\mathbb{R})$, alors sa *transposée* est ${}^tM = [m_{ji}]$.
– Si $M = [m_{i,j}] \in \mathcal{M}_n(\mathbb{C})$ On *étoile* est ${}^*M = {}^t\overline{M}$.

Proposition I.2. – La transposition/l'étoile est linéaire/antilinéaire et involutive.
– Pour $M, N \in \mathcal{M}_n(K)$, on a ${}^*(MN) = {}^*M{}^*N$.

Définition I.3. L'ensemble des matrices *symétriques* est $S_n(k) = \{M \in \mathcal{M}_n(\mathbb{R}) : {}^tM = M\}$ et l'ensemble des *matrices hermitiennes* est $H_n(\mathbb{C}) = \{M \in \mathcal{M}_n(\mathbb{R}) : {}^*M = M\}$.

• I.B Lien avec la dualité

Soit E un $\mathbb{R}$-espace vectoriel euclidien ou $\mathbb{C}$-espace vectoriel hermitien de dimension finie.

Définition I.4. – Pour $f \in L(E)$, l'adjoint de f est l'unique élément ${}^*f \in L(E)$ tel que $\forall x, y \in E, \langle x, fy\rangle = \langle {}^*fx, y\rangle$.
– On dit que f est auto-adjoint (ou symétrique dans le cas réel ou hermitienne dans le cas complexe) si ${}^*f = f$.

Proposition I.5. Soit (e) une base orthonormée et $f \in L(E)$ et M sa matrice et N la matrice de son adjoint.
– Alors ${}^*M = N$.
– f est auto-adjoint $\iff M$ est symétrie/hermitienne.

• I.C Lien avec les formes quadratiques

On rappelle qu'une forme hermitienne sur un $\mathbb{C}$-espace vectoriel E est une forme $f : E \times E \to \mathbb{C}$ antilinéaire à droite et linéaire à gauche et à symétrie hermitienne $(\forall x, y \in E, f(x, y) = \overline{f(y, x)}$. sa forme quadratique est alors à valeur réelle.

Proposition I.6. On a une bijection entre l'ensemble des f.b.s de $\mathbb{R}^n$ (resp. f.h de $\mathbb{C}^n$) et les matrices $S_n(\mathbb{R})$ (resp. $H_n(\mathbb{C})$).

Définition I.7. Si $A \in S_n^{++}(\mathbb{R})$, alors l'*ellipsoïde* centré en 0 associée à A est l'ensemble $E_A = \left\{{}^tXAX \leq 1\right\}$. Son *volume* $Vol(E_A)$ est sa mesure de Lebesgue. Son *déterminant* est le déterminant de A.

Théorème I.8. Développement [Ellipsoïdes de John] Si K est un compact d'intérieur non vide, alors il existe une unique ellipsoïde de volume minimal contenant K.

Applications I.9. Tout sous-groupe compacts de $GL_n(\mathbb{R})$ est conjugué à un sous-groupe de $O_n(\mathbb{R})$.

II Réduction des matrices symétriques et hermitiennes

• II.A Sous-espace propres et valeurs propres

Théorème II.1. Toute matrice symétrique réelle (resp. hermitienne) est diagonalisable en base orthonormées.

Applications II.2. Développement [Théorème de l'amitié] Soit G un graphe à n sommets tel que toute paire de sommets admet exactement un sommet adjacent commun. Alors il existe un sommet adjacent à tous les autres.

Théorème II.3 (Courant-Fisher)**.** Si f est auto-adjoint de valeurs propres $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Alors $\lambda_i = \min_{\dim F = i} \max_{x \in F} \frac{\langle x, f.x\rangle}{||x||^2}$.

Applications II.4. – ? ? ?
– Théorème d'entrelacement de Cauchy : Soit $f \in S_n(\mathbb{R})$ de valeurs propres $\lambda_1 \leq \cdots \leq \ldots \lambda_n$ et H un hyperplan. On note $\begin{array}{ccc} g : & H & \longrightarrow & H \\ & x & \longmapsto & \pi_H(f(x)) \end{array} \in S(H)$ et $\mu_1 \leq \cdots \leq \mu_{n-1}$ ses valeurs propres. Alors $\lambda_1 \leq \mu_1 \leq \lambda_2 \leq \cdots \leq \mu_{n-1} \leq \lambda_n$.

Théorème II.5. Soit $M \in S_n(\mathbb{R})$. Alors M est définie positive si et seulement si les mineurs principaux sont tous positifs.

III Racines carrés et décomposition polaires

Théorème III.1 (Racine carré)**.** L'application $\begin{array}{ccc} S_n^{++}(\mathbb{R}) & \longrightarrow & S_n^{++}(\mathbb{R}) \\ M & \longmapsto & M^2 \end{array}$ (resp. $\begin{array}{ccc} S_n^{++}(\mathbb{R}) & \longrightarrow & S_n^{++}(\mathbb{R}) \\ M & \longmapsto & M^2 \end{array}$) est un C^∞-difféormorphisme.

Proposition III.2 (Décomposition polaire)**.** L'application $\begin{array}{ccc} S_n^{++}(\mathbb{R}) \times O_n(\mathbb{R}) & \longrightarrow & GL_n(\mathbb{R}) \\ (S, O) & \longmapsto & SO \end{array}$ est un C^∞-difféomorphisme.

Applications III.3. – $O_n(\mathbb{R})$ est un sous-groupe compact maximal.
– Deux matrices réelles unitairement semblables sont orthogonalement semblables.

Théorème III.4. – L'application $\begin{array}{ccc} S_n & \longrightarrow & S_n^{++}(\mathbb{R}) \\ S & \longmapsto & exp(S) \end{array}$ est un C^∞-difféomorphisme.

– Si G est un sous-groupe de $GL_n(\mathbb{R})$ stable par adjonction tel que $G \cap S_n^{++}(\mathbb{R})$ est stable par racine carré, alors l'application
$\begin{array}{ccc} (G \cap S_n^{++}(\mathbb{R})) \times (G \cap O_n(\mathbb{R})) & \longrightarrow & G \\ (S, O) & \longmapsto & SO \end{array}$ est un C^∞-difféomorphisme.

Applications III.5. – Les groupeS $O(p, q)$ a 4 composantes connexes si $p, q \geq 1$.

– ? ? ?

IV Utilisation en analyse numérique

• IV.A Méthode du gradient conjugué

[A completer]

Développement

• IV.B Méthode de Jacobi de calcul de valeur propres

[A completer]

Développement

V Développements

– Théorème de l'amitié.
– Ellipse de John.
– Lemme de Morse.
– Méthode du gradient conjugué.
– Méthode de Jacobi.
– Décomposition polaire.
– Théorème de stabilité de Liapounov.
– Théorème d'Hermite.

Exercice .1. Théorème d'entrelacements de Cauchy.

Exercice .2. Montrer que pour $t \in [0, 1p$, $M(t) := [t^{|i-j|}]$ est définie positive.

131 - Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications

Références [Goblot, alg. lin.]

I Formes quadratiques

• I.A Définitions

Définition I.1. On note k un corps et E un k-esapce vectoriel de dimension n.
- Une *forme bilinéaire* sur E est une application $f : E \times E \to k$ linéaire en chaque variable.
- Elle symétrique si : $\forall x, y \in E, f(x,y) = f(y,x)$. Sa forme quadratique est $q(x) = f(x,x)$ et f est la forme polaire de q.
- Une forme quadratique q est non dégénérée si $\forall x \in E, (\forall y \in E, f(x,y) = 0) \implies x = 0$.

On note $Q(E)$ l'ensemble des formes quadratiques sur E.

Proposition I.2. Soit q une forme quadratique de forme polaire f.
- $\forall x, y \in E \forall \lambda \in k, q(x+y) = q(x) + 2f(x,y) + q(y)$ et $q(\lambda x) = \lambda^2 x$.
- Formule de polarisation : $\forall x, y \in E, f(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)) = \frac{1}{4}(q(x+y) - q(x-y))$. Donc si $q = 0$
- Soit $p : E \to k$, alors p est une forme quadratique si et seulement si : $\forall x \in E, \forall \lambda \in k, p(\lambda x) = \lambda x^2$ et $(x,y) \mapsto \dfrac{1}{2}(q(x+y) - q(x) - q(y))$ est bilinéaires.

Exemple I.3. Tout polynôme homogène de degré 2 est une forme quadratique.

• I.B Représentation matricielle

[A completer]

Définition I.4. Discriminant.

• I.C Endomorphismes remarquables

Définition I.5. Adjoint

Proposition I.6 (représentation matricielle)**.**

Définition I.7. Isométrie. Groupes orthogonal et special orthogonal.

II Isotropie et orthogonalité

• II.A Vecteurs isotropes et cône isotropes

On se donne q une forme quadratique et f sa forme polaire.

Définition II.1. Un vecteur x est dit *isotrope* si $q(x) = 0$. Le cône isotrope $C(q)$ est l'ensemble des vecteurs isotropes. Un sous-espace *totalement isotrope* (SETI) est un sous-espace constitué de vecteurs isotropes.

Proposition II.2.
- Le noyau est inclus dans le cône isotrope.
- Sur $\mathbb{R}$, si q est une forme quadratique positive, alors le cône isotrope est égal au noyau.

Applications II.3. Si E est un espace eucliden réel, alors tout endomorphisme symétrique est diagonalisable.

• II.B Quadriques projectives

• II.C Vecteurs orthognonaux et Théorème de Sylvester

Définition II.4.
- Deux vecteurs sont q-*orthognonaux* si $f(x,y) = 0$.
- Si F est un sous-espace, alors son orthogonal est $F^\perp = \{x \in E : \forall y \in F, f(x,y) = 0\} =$

Proposition II.5. Si q est non dégénéré, alors $\dim F = codim\ F$. Si de plus F n'a pas de vecteurs isotropes alors $F \oplus F^\perp = E$.

Exemple II.6. Si f est un produit sclaire sur $\mathbb{R}^n$, alors $F \oplus F^\perp$ pour tout sous-esapce F.

Théorème II.7 (Sylvester)**.** Tout forme quadratique admet une base de vecteurs orthogonaux. De façon équivalente : il existe une base $(\phi_i) i \in [1,n]$ de E^*, et des scalaires $(\lambda_i)_{i \in [1,n]}$ tels que $q = \sum_{i=1}^n \lambda_i \phi_i^2$.

Corollaire II.8 (Classification des formes quadratiques)**.**
- Sur un corps clos, deux formes quadratiques sont conjugués si et seulement si elles ont le même rang.
- Sur $\mathbb{R}$ les formes quadratique sont classées par leur signature.
- Sur $\mathbb{F}_q$, les forme quadratiques sont du type $diag(1, \dots, 1, 0, \dots)$, $diag(1, \dots, 1, a, 0, \dots)$, avec $a \in \mathbb{F}_q^2$.

III Classification des formes quadratiques

• III.A Théorème de Sylvester

Algorithme de Gauss.

• III.B Classification sur $\mathbb{R}$

Applications III.1.

• **III.C Classification sur un corps clos**

• **III.D Classification sur un corps fini**

IV Applications

• **IV.A Hessienne d'une application C^2**

Théorème IV.1 (Lemme de Morse)**.**

Applications IV.2. Lignes de niveaux

• **IV.B 1er et 2nd formes fondamentales**

Définition IV.3. $I(M)$ et $II(M)$.

Théorème IV.4 (Propriété de graphe)**.** .

• **IV.C Côniques et quadriques réelles**

Définition IV.5.

Théorème IV.6 (Classification)**.**

• **IV.D Espace des cercles-droites**

Définition IV.7. – Espace des cercles et des droites.
– Forme quadratique q.

Proposition IV.8. – q est de signature $(3,1)$.
– E est l'équation d'un cercle droite non dégénérée si et seulement si $q(E) > 0$.

Définition IV.9. Orthogonalité.

Proposition IV.10. E et E' sont orthogonaux pour q si et seulement s'ils sont orthogonaux géométriquement .

V Développements

– Théorème de l'amitié.
– Théorème de Stabilité de Liapounov.
– Sous-groupes compacts de $GL_n(\mathbb{R})$.
– Lemme de Morse.
– Théorème de John.
– $PSL_2(\mathbb{R}) \simeq O_0(2,1)$.
– Décomposition polaire.
– Décomposition d'Iwasawa.
– Théorème d'Hermite.
– Théorème de Fisher-Cochran.
– Quadriques dans $\mathcal{M}_2(\mathbb{R})$.

VI Exercice

Exercice .1 (Gourdon, Alg, Chap 5.1, Ex 5)**.** (SETIM) Soit q une forme quadratique de rang r et F un SETI. Montrer que $\dim F \leq n - r/2$.

On suppose que $r = n$. Montrer que tous les SETIM on même dimension. On appelle indice de q la dimension d'un SETIM.

Etudier le cas reél.

Démonstration. On rappelle le lemme suivant

Lemme VI.1. On a $\dim F + \dim F^\perp = n + \dim(F \cap \ker q)$.

Démonstration du lemme. Celà vient du fait que $F^\perp = (q.F)^\perp$ et que $\dim q.F = \dim F - \dim(F \cap \ker q)$. □

Si F est un SETI alors $\dim F \leq \dim f^\perp$, ce qui donne $2\dim F \leq n + \dim(F \cap \ker q) \leq 2n - r$.

Soit F_1 et F_2 deux SETIM et $F = F_1 \cap F_2$. Son note G_1 un supplémentaire de F dans F_1 et de même pour G_2.

Montrons que $G_1 \cap G_2^\perp$. Soit $G_1 \cap G_2^\perp$. Alors Kx est en somme directe avec F_2 et d'après les hypothèses, x est orthognal à x, F et G_2, donc $Kx \oplus F_2$ est un SETI, et comme F_2 est maximal on en déduit que $x = 0$.

Donc G_1 et $G_2^\perp$ sont en somme direct. Comme q est non dégénéré, on en déduit que $\dim G_1 \leq \dim G_2$. Par symétrie des rôles on en déduit que $\dim G_1 = \dim G_2$ puis que $\dim F_1 = \dim F_2$.

Soit q une forme quadratique sur $\mathbb{R}$ de signature (p,q). Supposons d'abord q est non dégénérée. Soit F un SETI. On prend G et H deux sous-espace supplémentaires orthogonaux tel que $q_{|G}$ est définie positive et $q_{|G}$ est définie négative. Comme Fest un SETI, on a $F \cap H = \{0\}$, donc par Grassmann $\dim F \leq \dim H = q$ et de même $\dim F \leq \dim G = p$. D'où $\boxed{\dim F \leq \min(p,q)}$.

Réciproquement on peut construire un SETI de dimension $\min(p,q)$, en considérant des bases othonormées de G et H.

Si q est dégénérée, alors en prend K un supplémentaire de $\ker q$. Si F est un SETIM, alors $\ker q \subset F$ et $F \cap K$ est un SETIM de $q_{|K}$ [y réfléchir]. Donc q est d'indice $\dim \ker q + \min(p,q) = n - \max(p,q)$. □

Exercice .2 (Gourdon, Alg, Chap 5.1, Ex 6)**.** Soit ϕ une forme bilinéaire telle que $\forall x, y \in E, {}^t x\phi y = 0 \iff {}^t y\phi x = 0$. Montrer que ϕ est symétrique ou antisymétrique.

Démonstration. L'hypothèse montre que pour tout $x \in E$, on a $\ker {}^t\phi \supset \ker \phi$, donc il existe $\lambda_x \in K$ tel que ${}^t\phi = \lambda_x \phi$. Le lemme suivant montre que λ_x est indépendant de x, et on en déduit que $\lambda = \pm 1$.

Lemme VI.2. Soient $f, g : E \to F$ telles que

$$\forall x \in E, \exists \lambda_x \in K, f.x = \lambda_x g.x.$$

Alors il existe λ tel que $f = \lambda g$.

Démonstration. On note K un supplémentaire de $\ker g$ et $h = g_{|K}$. Alors $h^{-1} \circ f : K \to K$ est une homothétie (on a $\Im f \subset \Im g$). On note λ son rapport et on a $f.x = \lambda g.x$ sur K et $f.x = g.x. = 0$ sur $\ker g$, d'où $f = \lambda g$. □

□

132 - Formes linéaires et hyperplans en dimension finie. Exemples et applications.

Références [? ? ?]

I Formes linéaires

• I.A Définitions et propriétés

On note E un sous-espace vectoriel de dimension finie sur un corps k.

Définition I.1. Le dual de E est $E^* = L(E,k)$. Une *forme linéaire* sur E est un élément de E^*.

Exemple I.2.
- $(x_1,\dots,x_n) \in k^n \mapsto x_1+\cdots+x_n$.
- $P(X) \in \mathbb{R}[X]_n \mapsto \int_0^1 P(t)dt$.
- $M \in \mathcal{M}_n(\mathbb{R}) \mapsto Tr(M)$.

Proposition I.3.
- On a $\dim E^* = \dim E$.
- Si ϕ est une forme linéaire non nulle, alors elle est surjective.

Applications I.4. Si $f : \Omega \to \mathbb{R}$ est C^1 et si sa différentielle ne s'annule pas, alors $f^{-1}(0)$ est une sous-variété.

• I.B Hyperplans

Définition I.5. Un *hyperplan* est le noyau d'une forme linéaire.

Proposition I.6.
- Un sous-espace vectoriel est un hyperplan si et seulement si il est de codimension 1.
- Si H est un hyperplan, alors toute droite non incluse dans H est un supplémentaire.

Proposition I.7. Tout sous-espace vectoriel de codimension r est intersection de r hyperplans indépandants.

Applications I.8. Si A est une k-algèbre de dimension fini et $\phi : A \to k$ un morphisme de k-algèbre, alors $\ker\phi$ est un idéal maximal (Théorème de ? ? : tout idéal maximal de $\mathbb{C}[X,Y]$ est de la forme $(X-a, Y-b)$).

II Dualité

• II.A Crochet de dualité et bases duales

Définition II.1. Le *crochet de dualité* sur E est l'application bilinéaire

$$\langle .,. \rangle_E : \begin{array}{ccc} E^* \times E & \longrightarrow & k \\ (\phi, x) & \longmapsto & \phi.x \end{array}.$$

Proposition II.2.
- Le crochet de dualité est une application bilinéaire non dégénérée.
- L'application $\begin{array}{ccc} E & \longrightarrow & E^{**} \\ x & \longmapsto & \langle .,x\rangle \end{array}$ est un isomorphisme.

Remarque II.3. L'espace E^{**} est alors canoniquement isomorphe à E. On dentifiera $\langle .,. \rangle_E$ et $\langle .,. \rangle_{E^*}$.

Exemple II.4. ? ? ?

Proposition II.5. Pour $(e_i)_{i\in[1,n]}$ une base de E, il existe une unique base $(e_i^*)_{i\in[1,n]}$ de E^*, telle que : $\forall i,j \in [1,n] e_i^*(e_j) = \delta_{i,j}$.

Définition II.6. La base $(e_i^*)_{i\in[1,n]}$ s'appelle la *base duale* de $(e_i)_{i\in[1,n]}$.

Proposition II.7. Dans les bases $(e_i)_{i\in[1,n]}$ et $(e_i)_{i\in[1,n]}$, la matrice du crohcet de dualité est I_n.

Applications II.8.
- Polynômes interpolateurs de Lagrange : pour $(x_1,\dots,x_n)$ des points distincts de $\mathbb{R}$, il existe une unique famille de polynômes $(P_1,\dots,P_n)$ de degré $\leq n-1$ tels que : $\forall i,j \in [1,n], P_i(x_j) = \delta_{i,j}$.
- Polynômes interpolateurs d'Hermite : pour $(x_1,\dots,x_n)$ des points distincts de $\mathbb{R}$ et $(k_1,\dots,k_n)$ des entiers, il existe une unique famille de polynômes $(P_{i,k})_{i\in[1,n],k\in[0,k_i-1]}$ de degré $\leq k_1+\cdots+k_n-1$ tels que : $\forall i \in [1,n], \forall k \in [0,k_i], P_{i,k}^{(l)}(x_j) = \delta(k,l).\delta_{i,j}$.

• II.B Transposition et orthogonalité

Définition II.9. Si $f \in L(E,F)$ sa transoposée est l'application

$${}^tf : \begin{array}{ccc} F^* & \longrightarrow & E^* \\ \phi & \longmapsto & \phi.f \end{array}.$$

On a alors : $\forall \phi \in F^*, \forall x \in E, \langle {}^tf.\phi, x\rangle_E = \langle \phi, f.x\rangle_F$.

Proposition II.10. La transposition est linéaire contravariante : si $f \in L(E,F)$ et $g \in L(F,G)$, alors ${}^t(g.f) = {}^tf.{}^tg$.

Définition II.11. On dit que $\phi \in E^*$ est orthogonal à x si $\phi.x = 0$.

Proposition II.12.
- Si H est un sous-espace stable par f, alors $H^\perp$ est stable par ${}^tf$.
- On a pour F sous espace de E ou E^* : $\dim F^\perp = codim\ F$ et $F^{\perp\perp} = F$.

Applications II.13. Si ${}^tf$ admet un vecteur propre, alors f admet un hyperplan stable (trigonalisation).

Applications II.14. Développement [Sous-espace stable par translation] Si E est un sous-espace vectoriel de dimension finie de $C^0(\mathbb{R},\mathbb{R})$ stable par translation, alors c'est l'espace des solutions d'une EDL à oefficients constants.

• II.C Cas d'un espace euclidien

On considère E un espace euclidien.

Théorème II.15 (Riesz ?)**.** L'application $\begin{array}{ccc} E & \longrightarrow & E^* \\ x & \longmapsto & \langle x, . \rangle \end{array}$ est un isomorphisme d'EVN.

Corollaire II.16. Tout hyperplan est du type $u^\perp$ avec u un vecteur unitaire.

Remarque II.17. Une base orthonormée est une base qui est sa propre bas duale.

Applications II.18. ? ? ?

Définition II.19. Une *réflexion* est un symétrie hyperplane.

Proposition II.20. Le groupe $O_n(\mathbb{R})$ est engendré par les réflexions.

III Application en géométrie

• III.A Hyperplans et convexité

Théorème III.1 (Hahn-Banach)**.** Si A et B sont deux convexes fermés, alors il existe H un hyperplan qui sépare strictement A et B.

Corollaire III.2.
- Un convexe fermé est l'intersection du tous les hperplans qui le contient.
- Si f est une fonction convexe, alors $f = sup_{u \leq f} u$ où u parcourt l'ensemble des fonctions affines $\leq f$.
- Soit A partie de E et $x \in A$. Alors $x \in \overline{Conv(A)} \iff \forall \phi \in E^*, \phi(x) \leq sup_{y \in A} \phi(y)$.

Applications III.3. Développement [Enveloppe convexe du groupe orthogonal] On munit $\mathcal{M}_n(\mathbb{R})$ de la norme 2 subordonnée. Alors $B(\bar{0}, 1)$ est l'enveloppe convexe de $O_n(\mathbb{R})$ et $O_n(\mathbb{R})$ est l'ensemble des points extrémaux de $B(\bar{0}, 1)$.

• III.B Dualité projective

Définition III.4. Si $E \mod \mathbb{R}^*$ est un sous-espace projectif de $P(\mathbb{R}^3)$, alors son dual est $\{\phi \mod \mathbb{R}^* \in P(\mathbb{R}^{3*}) : \forall x \in E \phi.x = 0\}$.

Proposition III.5.
- Le dual d'un point de $P(\mathbb{R}^3)$ est une droite de $P(\mathbb{R}^{3*})$.
- Le dual d'une droite de $P(\mathbb{R}^3)$ est un point de $P(\mathbb{R}^{3*})$.
- Si M est un point incidant à une droite D , alors $M^\perp$ est une droite contenant $D^\perp$.
- Les duaux de trois points alignés sont trois droite concourantes.

Exemple III.6. Théorèmes duaux :
- Menelaus/Ceva :...
- Desargue (autodual) : ...

Définition III.7. Si C est une conique de $P(\mathbb{R}^3)$ alors son dual est : $C^\perp = \{\phi \in P(\mathbb{R}^{3*}) : \phi^\perp$ est une droite tangente à $C\}$.

Proposition III.8. Si C est une conique propre associée à la forme quadratique Q, alors $C^\perp$ est une conique associé à la forme quadratqiue Q^{-1}.

Exemple III.9. Pascal/Brianchon : ...

IV Développements

- Théorème de Hahn-Banach.
- Enveloppe convexe du groupe orthogonal.
- Critère de nilpotence de Cartan.
- Sous-espace stable par translation.

133 - Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie)

Références [Arnaudies 3], [Tauvel], [Goblot].

I Adjonction et définitions

• I.A Définitions et propriétés

Définition I.1. Adjoint, transposéed'un matrice

Proposition I.2. Existence + invoultion + règle de calcul.

Définition I.3.
- Endomorphismes symétriques/autoadjoints, symétrique positive
- antisymétriques.
- orthogonaux, rotations
- normaux.
- Similitude vectorielle.

Proposition I.4. Représenation matricielle.

Proposition I.5. f^*f est symétrique positive (définie). Bijection avec les formes quadratiques

Proposition I.6. Noyau image de f^* et sous-espace stables.

Proposition I.7. $\|f\| = \max\langle x, f.x\rangle$

Théorème I.8. Développement Sous-groupes compacts.

• I.B Lien avec la dualité

[A completer]

• I.C Changement de base orthonormée

II Études des endomorphismes en espace euclidiens

• II.A Réduction des endomorphisme normaux

Théorème II.1. Reduction des endomrophismes normaux.

Proposition II.2.
- Structure de $SO_2(\mathbb{R})$.
- Endomorphisme orthogonaux.
- Endoorphisme antisymétrique.

Proposition II.3. $SO_n(\mathbb{R})$ est connexe.

• II.B Groupe orthogonal

Définition II.4. Symétries orthogonales, réflections.

Proposition II.5.
- Les réflection engendrent $O_n(\mathbb{R})$.
- Les retournements engendrent $SO_n(\mathbb{R})$.

• II.C Diagonalisation des endomorphismes symétriques

Théorème II.6. Toute matrice symétrique réelle (resp. hermitienne) est diagonalisable en base orthonormées.

Théorème II.7 (Courant-Fisher)**.** Si f est auto-adjoint de valeurs propres $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Alors $\lambda_i = \min_{\dim F = i} \max_{x \in F} \frac{\langle x, f.x\rangle}{||x||^2}$.

Applications II.8.
- ???
- Théorème d'entrelacement de Cauchy : Soit $f \in S_n(\mathbb{R})$ de valeurs propres $\lambda_1 \leq \cdots \leq \ldots \lambda_n$ et H un hyperplan. On note $g : \begin{array}{ccc} H & \longrightarrow & H \\ x & \longmapsto & \pi_H(f(x)) \end{array} \in S(H)$ et $\mu_1 \leq \cdots \leq \mu_{n-1}$ ses valeurs propres. Alors $\lambda_1 \leq \mu_1 \leq \lambda_2 \leq \cdots \leq \mu_{n-1} \leq \lambda_n$.

Théorème II.9. Soit $M \in S_n(\mathbb{R})$. Alors M est définie positive si et seulement si les mineurs principaux sont tous positifs.

Définition II.10. Si $A \in S_n^{++}(\mathbb{R})$, alors l'*ellipsoïde* centré en 0 associée à A est l'ensemble $E_A = \left\{ {}^tXAX \leq 1 \right\}$. Son *volume* $Vol(E_A)$ est sa mesure de Lebesgue. Son *déterminant* est le déterminant de A.

Théorème II.11. Développement [Ellipsoïdes de John] Si K est un compact d'intérieur non vide, alors il existe une unique ellipsoïde de volume minimal contenant K.

Applications II.12. Tout sous-groupe compacts de $GL_n(\mathbb{R})$ est conjugué à un sous-groupe de $O_n(\mathbb{R})$.

III Racines carrés et décomposition polaires

Théorème III.1 (Racine carré)**.** L'application $\begin{array}{ccc} S_n^{++}(\mathbb{R}) & \longrightarrow & S_n^{++}(\mathbb{R}) \\ M & \longmapsto & M^2 \end{array}$ (resp. $\begin{array}{ccc} S_n^{++}(\mathbb{R}) & \longrightarrow & S_n^{++}(\mathbb{R}) \\ M & \longmapsto & M^2 \end{array}$) est un C^∞-difféormorphisme.

Proposition III.2 (Décomposition polaire)**.** L'application $\begin{array}{ccc} S_n^{++}(\mathbb{R}) \times O_n(\mathbb{R}) & \longrightarrow & GL_n(\mathbb{R}) \\ (S, O) & \longmapsto & SO \end{array}$ est un C^∞-difféomorphisme.

Applications III.3.
- $O_n(\mathbb{R})$ est un sous-groupe compact maximal.
- Deux matrices réelles unitairement semblables sont orthogonalement semblables.

Théorème III.4. – L'application $\begin{array}{ccc} S_n & \longrightarrow & S_n^{++}(\mathbb{R}) \\ S & \longmapsto & exp(S) \end{array}$ est un C^∞-difféomorphisme.

– Si G est un sous-groupe de $GL_n(\mathbb{R})$ stable par adjonction tel que $G \cap S_n^{++}(\mathbb{R})$ est stable par racine carré, alors l'application $\begin{array}{ccc} (G \cap S_n^{++}(\mathbb{R})) \times (G \cap O_n(\mathbb{R})) & \longrightarrow & G \\ (S, O) & \longmapsto & SO \end{array}$ est un C^∞-difféomorphisme.

Applications III.5. – Les groupeS $O(p, q)$ a 4 composantes connexes si $p, q \geq 1$.

– ? ? ?

IV En dimension 3

• IV.A Groupe $SO_3(\mathbb{R})$

Théorème IV.1. Groupe des polyèdre et sous-groupes finis de $SO_3(\mathbb{R})$.

Définition IV.2. Groupes libres

Théorème IV.3. Développement [Banach-Tarski]

• IV.B Prodduit vectoriel

Définition IV.4. Produit vectoriel. produit mixte.

Proposition IV.5. Soit $u = (x, y, z)$.Alors la matrice de $u \wedge .$ est $\begin{bmatrix} 0 & -z & y \\ z & 0 & -x \\ -y & x & 0 \end{bmatrix}$.

Exemple IV.6. Equation vérifié par la courbure et la torsion.

Proposition IV.7. Les solutions de $X'(t) = u \wedge X(t)$ sont des cercles d'axe u.

V Développements

– Théorème de Banach-Tarski.
– Groupes des isométries de l'icosaèdre.
– Théorème de John.
– Sous-groupes compacts de $GL_n(\mathbb{R})$.
– Corps des quaternions.
– Décomposition polaire.

VI Exercice

135 - Isométries d'un espace affine euclidien de dimension finie. Forme réduite. Applications en dimensions 2 et 3.

Références [Arnaudies 3].

I Structure du groupe des isométries

II Définitions

On considère E un espace affine euclidien de direction $\vec{E}$ munie de la disatnce euclidienne.

Définition II.1. Une application $f : E \to E$ est une *isométrie* si elle conserve les distances. Leur ensemble est noté $Isom(E)$.

Proposition II.2.
- Toute isométrie est une application affine et sa direction est endomrophisme orthogonal.
- Une application affine est une isométrie si et seulement si sa direction est un endomorphisme orthogonal.
- $Isom(E)$ est une sous-groupe du groupe affine.

Exemple II.3.
- Toute translation est une isométrie.
- Une symétrie orthogonale (affine) par rapport à un sous-espace affine F, est l'application $s_F : E \to E$ telle que s_F fixe F points par points et $\vec{s_F}$ est la symétrie orthogonale par rapport à $\vec{F}$. Une *réflexion* est une isométrie par rapport à un hyperplan affine.

Proposition II.4. On a $Isom(E) \simeq \vec{E} \rtimes O(\vec{E})$.

Définition II.5. Le groupe des déplacements est $\left\{ f \in Isom(E) : \det \vec{f} = 1 \right\}$. Un *antidéplacement* est une isométrie f telle que $\det \vec{f} = -1$.

Proposition II.6 (Générateurs)**.**
- Les réflexions affines engendrent $Isom(E)$.
- Les retournements engendrent $Isom^+(E)$.

III Formes réduites

Définition III.1. Une application affine admet une *forme réduite* si elle se décompose de façon unique en un produit commutatif d'une translation et d'une application affine avec point fixe.

Théorème III.2 (Forme réduite)**.**
- Une application affine admet une forme réduite si et seulement si $\mathrm{Im}(\vec{f} - Id) \oplus \ker(\vec{f} - Id) = \vec{E}$.
- Toute isométrie admet une forme réduite.

IV Cas de la dimension 2 et 3

• IV.A Isométries en dimension 2

Proposition IV.1 (Classification)**.** Les isométries affines de $Isom(\mathbb{R}^2)$ sont à conjugaison près les suivants
- Les translations : ...
- Les rotations : ...
- Les réflexions : ...
- Les réflexions glissées : ...

Proposition IV.2 (Représentation complexe)**.** On se place dans $\mathbb{C}$.
- Les translations s'écrivent : $z \mapsto z + u$.
- La rotation de centre a et d'angle θ s'écrit : $z \mapsto e^{i\theta}(z - a) + a$.
- Les symétrie glissées s'écrivent : $z \mapsto e^{2i\theta}(\bar{z} - a) + a + u$.

Proposition IV.3. Un triangle abc est équilatéral directe si et seulement si $a + jb + j^2c = 0$.

Applications IV.4.
- Théorème de Napoléon : soit ABC un triangle, et PRQ les centres des triangles équilatéraux extérieurs à ABC. Alors PQR est un triangle équilatéral.
- Théorème de Morley : L'intersectection des trisectrices d'un triangle est un triangle équilatéral.
- Point de Fermat : le point F du plan qui minimise $AF + BF + CF$, vérifie $(FA, FB) = (FB, FC) = (FC, FA) = \frac{2\pi}{3}$.
- Droite de Steiner.

• IV.B Isométries en dimension 2

Proposition IV.5 (Classification)**.** Les isométries affines de $Isom(\mathbb{R}^3)$ sont à conjugaison près les suivants
- Les translations : ...
- Les rotations : ...
- Les vissages : ...
- Les réflexions : ...
- Les réflexions glissées : ...
- Les anti-rotations : ...

V Utilisation des isométries

• V.A Groupes des isométries des polyèdres

Définition V.1. Un polyèdre est *régulier* si toutes ses faces des polygônes isométriques, et l'ensemble des somemts adjacent à tout sommet s forment un polygône régulier.

Théorème V.2. Il existe 5 polyèdres réguliers.
- Le groupe des isométries du tétraèdre est isomorphe à $\mathfrak{A}_4$.
- Le groupe des isométries du cube/octaèdre est isomorphe à $\mathfrak{S}_4$.
- Développement Le groupe des isométries du dodécaèdre/icosaèdre est isomorphe à $\mathfrak{A}_5$.

Applications V.3. Dénombrement des coloriages du cube.

• V.B Sous-groupes finis de $O_2(\mathbb{R})$ et $SO_3(\mathbb{R})$

Applications V.4. Les sous-groupes finis de $SO_3(\mathbb{R})$ sont isomorphes à : $\mathbb{Z}/n\mathbb{Z}$, D_{2n}, $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$.

• V.C Duplication de la sphère

Définition V.5. Le *groupe libre* de rang 2, noté F_2, est l'ensemble des mots sur $\{a, a^{-1}, b, b^{-1}\}$, munie de la concaténation avec ε le mot vide et la règle $aa^{-1} = a^{-1}a = bb^{-1} = b^{-1}b = \varepsilon$.

Tout éléments de F_2 s'écrit de façon unique sous la forme $a^{\alpha_1}b^{\beta_1}\dots a^{\alpha_p}b^{\beta_p}$, avec $\alpha_i, \beta_i \in \mathbb{Z}^*$ et $\alpha_1, \beta_p \in \mathbb{Z}$.

Théorème V.6. Développement [Banach-Tarski faible] Il existe :
- D une partie dénombrable au plus de $\mathbb{S}^2$.
- Une partition de $\mathbb{S} \setminus D$ en 4 partie : $\mathbb{S} \setminus D = A_1 \sqcup A_2 \sqcup A_3 \sqcup A_4$
- Deux rotations $f, g \in SO_3(\mathbb{R})$.

Tels que

$$\mathbb{S}^2 \setminus D = A_1 \sqcup a(A_2) = A_3 \sqcup b(A_4).$$

VI Groupe des paveurs

Définition VI.1. Un pavage du plan euclidien E est un couple (P, G) où P est un compact d'intérieur non vide de E et G un sous-groupe de $Isom^+(E)$ vérifiant :
- $E = \bigcup_{g \in G} g(P)$.
- Pour tout $g, h \in G$, si $int(g(P)) \cap int(h(P)) \neq \emptyset$, alors $g(P) = h(P)$.

Théorème VI.2. Il existe cinq types de pavages à conjugaison près dans $Isom^+(E)$.

VII Développements

- Théorème de Banach-Tarski.
- Groupe des isométrie des polyèdres.
- Corps des quaternions.
- Groupes de pavages.
- Sous-groupes compact de $GL_n(\mathbb{R})$

Exercice .1 (Ladegaillerie, Chap II, Sec 2.5, Ex 1)**.** Soient A, B deux points du plan et Δ, Δ' deux droites concourantes. Sachant que l'on a une règle et que l'on sait tracer des parallèles, construire les points C et D tels que $C \in \Delta$ et $D \in \Delta'$ et $ABCD$ soit un parallélogramme.

Démonstration. On trace la parallèle à Δ passant par A et la parallèle à Δ' passant par B. On obitent alors un parallélogramme dont le centre est noté O. Le point C est alors $\Delta \cap (AO)$ et D est $\Delta' \cap (BO)$. □

136 - Coniques. Applications

Références [Berger 4], [Tauvel], [Goblot], [Arnaudies].

Introduction

I Coniques

• I.A Propriétés des coniques affines

On se place dans E un plan affine de direction $\vec{E}$.

Définition I.1. Un *polynôme de degré* 2 sur P est une application $f : P \to \mathbb{R}$ tel qu'il existe $O \in E$, q une forme quadratique sur $\vec{E}$, L une forme linéaire et c une constantes tel que : $f(M) = q(\overrightarrow{OM}) + L.\overrightarrow{OM} + C$.

Proposition I.2. Si $f(M) = q(\overrightarrow{OM}) + L.\overrightarrow{OM} + C$ et si O' est un autre poit alors : $f(M) = q(\overrightarrow{O'M}) + (L + 2{}^t\overrightarrow{OO'}.q).\overrightarrow{O'M} + C + q(\overrightarrow{OO'}) + L.\overrightarrow{OO'}$.

Remarque I.3.
- La forme quadratique q ne dépend pas du point O.
- Si $E = \mathbb{R}^2$ celà revient à dire que f est un polynome de degré 2 de $\mathbb{R}[X, Y]$.

Définition I.4. La *conique* associée à f est l'ensemble de ses zéros.

Remarque I.5. Si deux polynômes de degréf, g diffèrent d'une constante multiplicative non nulle, alors ils définissent la même conique.

Exemple I.6. ? ? ?

Définition I.7. Un point O est centre de la conique associcée à f si $L = 0$. Une conique est dite *à centre* si elle admet un unique centre.

Proposition I.8. Une conique est à centre si et seulement si q est non dégénérée.

Exemple I.9 (A completer)**.** .

II Lien avec les quadriques projective de $P^2(\mathbb{R})$

Définition II.1. Si F est un polynôme homogène de degré 2 sur $\mathbb{R}^3$, alors la *quadrique* associée à F est l'ensemble des $M = [x : y : z] \in P^2(\mathbb{R})$ tel que $F(x, y, z) = 0$ (indépendant du ds coordonnés homogènes de M).

Exemple II.2.
- $x^2 + y^2 + z^2$ donne une quadrique vide.
- $x^2 + y^2 - z^2$ donne une quadrique non triviale.

Remarque II.3.
- Si on multiplie F par une constante non nulle, alors on ne change pas sa quadrique.
- A changement de base près il existe qu'une seule quadrique non dégénérée et non vide : $x^2 + y^2 - z^2$.

On prend $E = \mathbb{R}^2 \times \{1\} \subset \mathbb{R}^3$.

Définition II.4.
- Si $f(x, y, 1) = Q(x, y) + L(x, y) + c$ est un polynôme de degré 2 sur E, alors son homogénéisé est la forme quadratique sur $\mathbb{R}^3$: $Q(x, y, z) = z^2 f(x/z, y/z, 1) = Q(x, y) + zL(x, y) + z^2 c$.
- La conique associée à f est dite propre si Q est non dégénérée et si sa coniaue est non vide.

Proposition II.5. On a $\{M \in E : f(M) = 0\} = \{M \in \mathbb{R}^3 : Q(M) = 0\} \cap E$.

Remarque II.6. Donc une conique propre est l'intersection d'un cône et d'un hyperplan affine ne passant pas par 0.

III Classification des coniques

• III.A Classification affine

Pour simplifier on prend $E = \mathbb{R}^2$ en tant qu'espace affine. On fait agir $GA(E) \times \mathbb{R}^*$ sur l'ensemble $\mathbb{R}[X, Y]_2$ par : $(u, \lambda).f = \lambda f \circ u^{-1}$. Celà correspond à un changement de repère et d'une multiplication par un scalaire.

Proposition III.1 (Classification affine)**.** Les orbites sont entièrement déterminés par les signature à échange près. Les représentants des orbites pour cette action sont :
- $x^2 + y^2$ si $\varepsilon(q) = (2, 0)$ et $\varepsilon(Q) = (2, 0)$.
- $x^2 + y^2 + 1$ si $\varepsilon(q) = (2, 0)$ et $\varepsilon(Q) = (3, 0)$.
- $x^2 + y^2 - 1$ si $\varepsilon(q) = (2, 0)$ et $\varepsilon(Q) = (2, 1)$.
- x^2 si $\varepsilon(q) = (1, 0)$ et $\varepsilon(Q) = (1, 0)$.
- $x^2 + 1$ si $\varepsilon(q) = (1, 0)$ et $\varepsilon(Q) = (2, 0)$.
- $x^2 - 1$ si $\varepsilon(q) = (1, 0)$ et $\varepsilon(Q) = (1, 1)$.
- $x^2 - y$ si $\varepsilon(q) = (1, 0)$ et $\varepsilon(Q) = (2, 1)$.
- $x^2 - y^2$ si $\varepsilon(q) = (1, 1)$ et $\varepsilon(Q) = (1, 1)$.
- $x^2 - y^2 + 1$ si $\varepsilon(q) = (1, 1)$ et $\varepsilon(Q) = (2, 1)$.

Remarque III.2. Il n'y a que 3 coniques propres à changement de repère près :
- $x^2 + y^2 - 1$: ellipse qui est à centre.
- $x^2 - y^2 + 1$: hyperbole qui est à centre.
- $x^2 - y$: parabole qui n'est pas à centre.

IV Classification euclidienne

Proposition IV.1 (Classification euclidienne)**.** Si on munie $\mathbb{R}^2$ de sa structure euclidiennes et si on fait agir $GO(\mathbb{R}^2) \times \mathbb{R}^*$ sur l'ensemble des coniques propres, alors les orbites son donnés par :
- $\frac{x^2}{a^2} + \frac{y^2}{b^2} - 1$: ellipse. C'est un cercle si $a = b$.

– $\frac{x^2}{a^2} - \frac{y^2}{b^2} - 1$: hyperbole. C'est une hyperbole équilatère si $a = b$.
– $x^2 - 2py$: parabole.

V Propriétés des coniques

• V.A Propriétés focales

[A completer]

• V.B Propriétés affines et métriques des conique

[A completer]

VI Développements

– Mouvement des planètes.
– Théorème de Pascal.
– Théorème de Poncelet.

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

Références [...]

I Barycentre en espace affine

• I.A Fonction vectorielle de Leibniz

On considère E un espace affine réel de dimension finie de direction $\vec{E}$.

Définition I.1. Soient $(M_i, \lambda_i)_{i\in[1,n]}$, un sytème de points pondérés. La fonction vectorielle de Leibniz est

$$\begin{array}{rccc} F: & E & \longrightarrow & \vec{E} \\ & M & \longmapsto & \displaystyle\sum_{i=1}^{n} \lambda_i \overrightarrow{MA} \end{array}.$$

Proposition I.2. Si $\sum_{i=1}^n \lambda_i = 0$, alors F est constante. Si $\sum_{i=1}^n \lambda_i \neq 0$, alors F est bijective.

Définition I.3. Si $\sum_{i=1}^n \lambda_i \neq 0$, alors le barycentre de $(M_i, \lambda_i)_{i\in[1,n]}$ est l'unique point G de E tel que $F(G) = \vec{0}$. On note alors $G = \dfrac{1}{\sum_{i=1}^n \lambda_i} \displaystyle\sum_{i=1}^{n} \lambda_i M_i$.

Exemple I.4.
- Si $G = bar\{(A,\lambda),(B,\mu)\}$, alors $G \in (AB)$ et $\overrightarrow{AG} = \dfrac{\mu}{\lambda+\mu}\overrightarrow{AB}$.
- Si $G \in (AB)$, alors $G = bar\{(A, GB), (B, GA)\}$ (les longueurs sont comptés algébriquement).
- Si les λ_i sont égaux, alors G est l'isobarycentre des $(M_i)_{i\in[1,n]}$.

Remarque I.5. Si E est un sous-espace affine d'un espace vectoriel, alors la notation $G = \dfrac{1}{\sum_{i=1}^n \lambda_i} \displaystyle\sum_{i=1}^{n} \lambda_i M_i$ est cohérente avec l'addition.

• I.B Propriétés affines du barycentre

Proposition I.6. Si $G = bar\{(A_i,\lambda)_{i\in[1,n]}\}$, on a pour tout point O : $\overrightarrow{OG} = \displaystyle\sum_{i=1}^{n} \lambda_i \overrightarrow{OA_i}$ et $\overrightarrow{A_1G} = \dfrac{\sum_{i=2}^n \lambda_i \overrightarrow{A_1A_i}}{\sum_{i=1}^n \lambda_i}$.

Proposition I.7. Une partie F de E est un sous-espace affine si et seulement si elle est stable par barycentre.

Proposition I.8. Une application $f : E \to F$ est affine si et seulement si elle conserve le barycentre.

Proposition I.9 (Associativité)**.** Si $G = bar\{(A_1,\lambda_1),(A_2,\lambda_2),(A_3,\lambda_3)\}$ et $H = bar\{(A_1,\lambda_1),(A_2,\lambda_2)\}$, alors $G = bar\{(H, \lambda_1+\lambda_2),(A,\lambda_3)\}$.

Applications I.10. Ceviennes dans un triangle : soit ABC un triangle.
- L'isobarycentre d'un triangle est au 2/3 des médianes.
- Si I est centre du cercle inscrit, alors $I = bar\{(A, BC),(B, CA),(C, AB)\}$.
- Si O est centre du cercle circonscrit, alors $O = bar\{(A, \sin 2A),(B, \sin 2B),(C, \sin 2C)\}$.
- Si H est l'orthocentre, alors $H = bar\{(A, \tan A),(B, \tan B),(C, \tan C)\}$.

• I.C Applications aux repères affines

Pour $n \in \mathbb{N}$, on note $T_n = \{(x_1,\dots,x_{n+1}) \in \mathbb{R}^n : x_1 + \cdots + s_n = 1\}$. Si $(A_1,\dots,A_{n+1})$ est une famille de point de E, on considère l'application :

$$\begin{array}{rccc} & T_n & \longrightarrow & E \\ & (x_1,\dots,x_{n+1}) & \longmapsto & \displaystyle\sum_{i=1}^{n+1} x_i A_i \end{array}.$$

Proposition I.11. Cette application est affine et le sous-espace affine engendré par $(A_i)_{i\in[1,n]}$ est l'image cette application.

Définition I.12. On dit que $(M_1,\dots,M_{n+1})$ est un *repère affine* de E si cette application est bijective. Auquel cas l'antécédent d'un point s'appelle ses *coordonées barycentriques.*

Proposition I.13.
- Equations barycentriques des droites : $ax + by + cz = 0$.
- Equations barycentriques des coniques : $ax^2 + by^2 + cz^2 + dxy + exy + yz = 0$.

Applications I.14. Développement [Théorème de Pascal] Soient A, B, C, A', B', C', 6 points du plan (affine ou projectif) tels que 3 quelconques d'entre eux ne sont jamais alignés. On note $P = (BC')\cap(B'C)$, $Q = (CA')\cap(C'A)$, $R = (AB')\cap(A'B)$ (éventuellement à l'infini). Alors les 6 points (A, B, C, A', B', C') sont sur une conique si et seulement si les 3 points (P, Q, R) sont alignés (éventuellement sur la droite à l'infini).

II Ensembles convexes

• II.A Définitions et propriétés

Définition II.1. Un partie convexe de E est une partie X telle que si $A, B \in X$, alors $\forall t \in [1,t], tA + (1-t)B \in X$.

Proposition II.2. Une X partie X est convexe si et seulement si elle est stable par barycentre à coefficients positifs.

Exemple II.3.
- Les intervalles sont les partie convexes de $\mathbb{R}$.
- Les boules sont des parties convexes.

Proposition II.4. – L'intersection de convexes est convexe.
– La fermeture d'un convexe est convexe.
– Si F est un convexe fermée, alors la distance de $x \in E \setminus F$ est atteinte en un seul point.

• II.B Enveloppes convexes

Définition II.5. L'*enveloppe convexe* d'une partie X est le plus petit convexe contenant X.

Théorème II.6. – L'enveloppe convexe de X est l'ensemble des barycentres à coefficients positifs des points de X.
Caratheodory Si $\dim E = N$, alors l'enveloppe convexe de X est l'ensemble des barycentres à coefficients positifs d'au plus $N+1$ points de X.

Exemple II.7. Gauss-Lucas : les racines de $P'(X)$ sont dasn l'enveloppe convexe des racines de P.

Définition II.8. Soit X, un ensemble. Un point $M \in X$ est extremal si pour $[A, B] \subset X$ et $M \in [A, B]$, on a $M = A$ ou $M = B$. .

Théorème II.9 (Krein-Milmann)**.** Si K est un convexe compact, alors c'est l'enveloppe convexe de ces points extremaux.

Exemple II.10. Les point extremaux de l'ensemble des matrices bisochastiques sont le matrice de permutation.

Théorème II.11. Développement [Enveloppe convexe du groupe orthogonal] L'ensemble $O_n(\mathbb{R})$ est l'ensemble des points extremqux de la boule fermée unité de $\mathcal{M}_n(\mathbb{R})$ pour la norme subordonnée à la norme 2.

Théorème II.12 (Lemme de Kakutani)**.** L'enveloppe convexe d'un compact est compact.

• II.C Caractérisations des convexes

Théorème II.13 (Hahn-Banach)**.** Si X et Y sont deux parties convexes (resp. convexes fermés), alors il existe un hyperplan qui sépare X et Y au sens large (resp. au sens strict).

Applications II.14. Jauge d'un conxexe.

Théorème II.15. Une partie X est convexe si et seulement si : pour tout $M \in E \setminus X$, il existe un hyperplan qui sépare X et M au sens large.

Corollaire II.16. Une partie fermée X est convexe si et seulement si : pour tout $x \in E \setminus F$, et $f \in F$ tel que $dist(x, F) = dist(x, f)$, on a : $\forall y \in x + \mathbb{R}_+(x - f), dist(y, F) = dist(y, f)$.

Théorème II.17. Développement [Théorème de Motkinz] Soit F une partie fermée. Si pour tout $x \in E \setminus X$ la distance $dist(x, F)$ est atteinte en un seul point, alors F est convexe.

• II.D Dual d'un convexe

Définition II.18 (A completer)**.**

Applications II.19. Polyèdres [A completer].

III Barycentre en dimension 2

On se place dans un plan affine E munie d'un repère affine.

Proposition III.1. Soient $A(x_a, y_a, z_a), B(x_b, y_b, z_b), C(x_c, y_c, z_c)$ trois point de E. Alors A, B, C sont alignés si et seulement si $\det \begin{pmatrix} x_a & x_b & x_c \\ y_a & y_b & y_c \\ z_a & z_b & z_c \end{pmatrix} = 0$.

Proposition III.2. L'équation barycetrique d'une droite de E est de la forme $ax + by + cz = 0$ avec $(a, c, b) \notin vect(1, 1, 1)$.

Théorème III.3 (Ménélaüs)**.** On se place dans un plan affine. On se donne ABC un triangle non plat et $M \in (BC)$, $N \in (CA)$, $P \in (AB)$ distincts de A, B, C. Alors

$$M, N, P \text{ sont alignés} \iff \frac{\overline{MB}}{\overline{MC}} \frac{\overline{NC}}{\overline{NA}} \frac{\overline{PA}}{\overline{PB}} = 1.$$

Théorème III.4 (Ceva)**.** On se place dans un plan affine. On se donne ABC un triangle et $M \in (BC)$, $N \in (CA)$, $P \in (AB)$ distincts de A, B, C. Alors

$$(AM), (BN), (CP) \text{ sont concourantes} \iff \frac{\overline{MB}}{\overline{MC}} \frac{\overline{NC}}{\overline{NA}} \frac{\overline{PA}}{\overline{PB}} = -1.$$

Exemple III.5. Ceviennes dans un triangle : soit ABC un triangle.
– L'isobarycentre d'un triangle est au 2/3 des médianes.
– Si I est centre du cercle inscrit, alors $I = bar\{(A, BC), (B, CA), (C, AB)\}$.
– Si O est centre du cercle circonscrit, alors $O = bar\{(A, \sin 2A), (B, \sin 2B), (C, \sin 2C)\}$.
– Si H est l'orthocentre, alors $H = bar\{(A, \tan A), (B, \tan B), (C, \tan C)\}$.

IV Utilisation de la convexité en analyse

• IV.A Théorèmes de points fixes

Théorème IV.1. (Théorème du point fixe de Kakutani) Soit K convexe compact de $\mathbb{R}^n$ et $(u_i)_{i \in I}$ une famille commutative de $\mathcal{M}_n(\mathbb{R})$ préservant K. Alors l'ensemble des points fixes communs de $(u_i)_{i \in I}$ dans K est un onvexe compact non vide.

Théorème IV.2. Développement Si G est un sous-groupe compact de $GL_n(\mathbb{R})$ et si K est un convexe compact de $\mathbb{R}^n$ tel que $G.K \subset K$, alors $\exists x_0 \in K, \forall g \in G, g.x = x$.

Applications IV.3. Si G est un sous-groupe compact de $GL_n(\mathbb{R})$, alors G est conjugué à un groupe de $O_n(\mathbb{R})$.

• IV.B Problèmes d'extremum

Définition IV.4. Soit X une partie convexe de $\mathbb{R}^n$. Une fonction $f : X \to \mathbb{R}$ est *convexe* (resp. strictement convexe) si son epigraphe est convexe (resp. strictement convexe).

Proposition IV.5. Si f est une fonction strictement convexe, alors f admet un unique minimum.

Exemple IV.6.
- Ensemble de niveau d'une fonction convexe.
- Plus grande valeur propre dans $S_n^{++}(\mathbb{R})$.
- ???

Applications IV.7. Développement [Point de Fermat] On considère E un plan euclidien et ABC un triangle dont tous les angles sont strictement inférieurs à $2\pi/3$. On définit la fonction

$$\begin{array}{rccc} f: & E^3 & \longrightarrow & \mathbb{R} \\ & (A,B,C) & \longmapsto & MA+MB+MC \end{array}.$$

On a les propriété suivantes
- La fonction f atteint un unique minimum, appelé point de Fermat, noté F.
- Le point F vérifie $\widehat{AFB} = \widehat{BFC} = \widehat{CFA} = 2\pi/3$.
- Si A' est tel que $A'BC$ est équilatéral extérieur, idem pour B' et C', alors F est l'intersection des segments $[A, A'], [B, B'], [C, C']$.
- Le point F est sur les cercles circonscrits de $A'BC$, $AB'C$ et ABC'.

Applications IV.8. Développement On considère E un espace euclidien. Si $q \in Q^{++}(E)$ est une forme quadratique définie positive, alors l'*ellipsoïde* centré en 0 associée à q est l'ensemble

$$E_q = q^{-1}([0,1]).$$

- Son volume $Vol(q)$ est sa mesure de Lebesgue.
- Son déterminant est le déterminant de sa matrice dans une base orthonormée. C'est aussi le détermiant de $A_q \in S^{++}(E)$ son endomorphisme autoadjoint associé.

[John] Si K est un compact d'intérieur non vide, alors il existe une unique ellipsoïde de volume minimal contenant K.

V Développements

- Sous groupes compacts.
- Théorème de Motkinz.
- Enveloppe convexe du groupe orthogonal.
- Théorème de John.
- Théorème de Pascal.
- Point de Fermat.

VI Exercices

Exercice .1. Soit X un fermé convexe d'intérieur non vide. Montrer que $X = adh(int(X))$.

Exercice .2 (Audin, Geo, Chap 1, Ex 1.6)**.** Soit E un espace affine et F une partie de E. Montrer que F est un sous-espace affine si et seulement si : $\forall A, B \in G, (AB) \subset F$.

Démonstration. Si $\forall A, B \in G, (AB) \subset F$, on montre que F est stable par barycentre par récurrence sur le nombre de points. □

Exercice .3 (Audin, Geo, Chap 1, Ex 1.23)**.** Soit $f : E \to E$ une application affine qui transforme une droite en une droite qui lui est parrallèle. Montrer que f est une homothétie ou une translation.

Démonstration. L'application $\vec{f}$ envoie toute droite vectoriel sur elle même, donc c'est une homothétie. □

Exercice .4 (Audin, Geo, Chap 1, Ex 1.24)**.** Montrer qu'une partie bornée ne peut avoir plus 'dun centrede symétrie.

Démonstration. Si X a deux centres de symétrie A, B, alors X est stable par $S_A \circ S_B = t_{2\overrightarrow{AB}}$, donc est non borné. □

Exercice .5 (Audin, Geo, Chap 1, Ex 1.36)**.** Déterminer le groupe affine d'une droite affine.

Démonstration. Soit D une droite et G son groupe affine. On prend O un point de D et on note : T le groupe des translations préservant D et H le sous groupe de G fixant O. On vérifie alors que $G = T \rtimes H$, et le groupe H est isomorphe au sous-groupe linéaire préservant une droite vectoriel (ce sont les matrices triangulaires par bloc 2×2, avec des blocs de taille 1 et $n-1$). □

Exercice .6 (Audin, Geo, Chap 1, Ex 1.42)**.** Soit $ABCD$ un quadrilatère. On considère A', B', C', D' les mileux des triangles ABC, ABD, BCD. Montrer que $ABCD$ et $A'B'C'D'$ sont homothétiques.

Démonstration. Soit D une droite et G son groupe affine. On prend O un point de D et on note : T le groupe des translations préservant D et H le sous groupe de G fixant O. On vérifie alors que $G = T \rtimes H$, et le groupe H est isomorphe au sous-groupe linéaire préservant une droite vectoriel (ce sont les matrices triangulaires par bloc 2×2, avec des blocs de taille 1 et $n-1$). □

Exercice .7 (Combes, Chap 7.9, Ex 2)**.** Soit C une partie convexe de $\mathbb{R}^2$, montrer que $Ext(C)$ est un fermé C. Montrer que c'est faux pour une partie convexe de $\mathbb{R}^3$.

138 - Homographies de la droite projective complexe. Applications.

Références [...]

I L'espace $P^1(\mathbb{C})$

• I.A Structure de la droite projective

Définition I.1. L'espace $P^1(\mathbb{C})$ est $\mathbb{C}^2 \setminus \{0\}/\mathbb{C}^*$ l'ensemble des droites complexes de $\mathbb{C}^2$. On note $\hat{\mathbb{C}} = \mathbb{C} \sqcup \{+\infty\}$. On a alors une bijection $\begin{array}{ccc} P(\mathbb{C}^1) & \longrightarrow & \hat{\mathbb{C}} \\ (x:y) & \longmapsto & x/y \end{array}$.

Proposition I.2. L'espace $P^1(\mathbb{C})$ est un espace compact homéomorphe à $\mathbb{S}^2$.

Définition I.3. Carte affine.

• I.B Homographies de $P^1(\mathbb{C})$

Proposition I.4. L'action de $GL_2(\mathbb{C})$ sur $\mathbb{C}^2$ passe quotient et induit une action sur $P^1(\mathbb{C})$ de noyau $\mathbb{C}^*$.

Définition I.5. Le groupe des homographies est : $PGL_2(\mathbb{C}) = GL_2(\mathbb{C})/C^*$.

Si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mod $\mathbb{C}^*$, alors pour $z \in \hat{\mathbb{C}}$, on a : $\gamma.z = \dfrac{az+b}{cz+d}$.

Proposition I.6.
- Le groupe $PGL_2(\mathbb{C})$ agit transitivement sur $P^1(\mathbb{C})$.
- Les homographie qui conservent le point ∞ sont exactement les homographies su type : $z \mapsto az + b$.

Proposition I.7. Le groupe $PGL_2(\mathbb{C})$ est engendré par :
- Les homothéties : $z \mapsto rz$ avec $r > 0$.
- Les rotations : $z \mapsto e^{i\theta}z$.
- Les translations : $z \mapsto z + a$, $a \in \mathbb{C}$.
- L'inversion : $z \mapsto z^{-1}$.

Proposition I.8. Une homographie a 1 ou 2 points fixes. Si elle en a qu'un, alors elle conjuguée à une translation, et si elle en a 2, alors elle est conjugué à une homothétie (de $P^1(\mathbb{C})$).

Applications I.9. Développement Étude des suites homographiques.

II Birapport

• II.A Repère projectif et birapport

Proposition II.1. Soit $P(E)$ un espace projectif complexe de dimension 1. Si a, b, c sont trois points distincts de $P(E)$, alors il existe une unique homographie $f : P(E) \to P^1\mathbb{C} = \hat{\mathbb{C}}$ tel que $f(a) = 0$, $f(b) = \infty$, $f(c) = 1$, .

Définition II.2. On dit qu (a, b, c) est un *repère projectif* de $P(E)$ et l'image d'un point $M \in P(E)$ par f sont ses *coordonnées homogènes*.

Définition II.3. Soient $(a, b, c) \in P(E)$ distincts et $D \in P(E)$. Le *birapport* $[a, b, c, d]$ est l'image de d par f.

Proposition II.4. Le groupe $PGL_2(\mathbb{C})$ agit simplement transitivement sur les repères et conserve le birrapport.

Proposition II.5. Si $a, b, c, d \in \mathbb{C}$, avec (a, b, c) distincts, alors : $[a, b, c, d] = \dfrac{d-a}{d-b} / \dfrac{c-a}{c-b}$.

III Cercles-droites

Proposition III.1. Si (a, b, c) sont trois points distincts de $\mathbb{C}$, alors l'ensemble $\{z \in \hat{\mathbb{C}} : [a, b, c, z] \in \hat{\mathbb{R}}\}$ est :
- le cercle passant par (a, b, c) si (a, b, c) ne sont pas aligné.
- la droite (a, b) union ∞ si (a, b, c) sont alignés.

Remarque III.2. Une droite est un cerlce passant par le point ∞.

Définition III.3. Soit $P(E)$ un espace porjectif de demension 1. Un *cercle-droite* de $P(E)$ est un ensemble X tel qu'il existe $(a, b, c) \in P(E)$ distincts tels que $X = \{z \in P(E) : [a, b, c, z] \in \hat{\mathbb{R}}\}$.

Remarque III.4. De façon équivelent un cercle-droite est l'image de $P^1(R)$ par une homographie $f : P^1(\mathbb{C}) \to P(E)$.

Proposition III.5. Le groupe $PGL(E)$ permute les cercles-droites.

Applications III.6 (Alternative de Steiner)**.** ...

• III.A Formule des 6 birapports

Théorème III.7 (6 birapport)**.** ...

Applications III.8.
- Droite de Simson : ...
- Théorème de Miquel : ...
- Théorème du pivot : ...

IV Groupe circulaire

• IV.A Symétries et inversion géométriques

Définition IV.1.
- Une *symétrie* est une réflexion r de $\mathbb{C}$ prolongée par $r(\infty) = \infty$.
- Une inversion géométrique est une application : $h_{O,k}(M) = O + k\dfrac{\overrightarrow{OM}}{OM^2}$, $h_{O,k}(\infty) = O$, avec $O \in \mathbb{C}$ et $k \in \mathbb{R}^*$.

Exemple IV.2.
- $z \mapsto \bar{z}$ est la symétrie d'axe $\mathbb{R}$.
- $z \mapsto \bar{z}^{-1}$ est l'inversion de centre O et de rapport 1.

Définition IV.3. Le groupe circulaire G est le groupe engendré par les homographies et $z \mapsto \bar{z}$.

V Propriétés du groupe circulaire

Proposition V.1.
- On a $G = PGL_2(\mathbb{C}) \rtimes \{z, \bar{z}\}$.
- Tout éléments de $G \setminus PGL_2(\mathbb{C})$ s'écrit $z \mapsto \gamma.\bar{z}$, avec $\gamma \in PGL_2(\mathbb{C})$.
- Le groupe cirulaire est engendré par les symétries et les inversions.

Proposition V.2.
- Tout élément du groupe circulaire transforme cercle-droite en un cercle droite.
- Si une application envoie un cercle-droite sur un cercle-droite, alors c'est une homographie.

Applications V.3. Développement $PSU_2(\mathbb{C}) \simeq SO_3(\mathbb{R})$.

VI Géométrie hyperbolique

• VI.A Action du groupe modulaire

Le *groupe modulaire* $SL_2(\mathbb{Z})$ agit sur $\mathcal{H}$ par homographie : pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ et $z \in \mathcal{H}$, l'action es donnée par : $\gamma.z = \dfrac{az+b}{cz+d}$.

On note $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Proposition VI.1. Le groupe modulaire est engendré par S, T.

Proposition VI.2. Un domaine fondamental est donné par $\{z \in \mathcal{H} \mid Re(z) \in [-1/2, 1/2], |z| \geq 1\}$.

Définition VI.3. Un *réseau* de $\mathbb{C}$ ou *tore complexe* est un sous-groupe du type $\Lambda = \mathbb{Z}u \oplus \mathbb{Z}v$, avec u, v deux vecteurs libres sur $\mathbb{R}$. Deux réseaux Λ_1, Λ_2 sont dit isomorphes s'il existe $a \in \mathbb{C}$ tel que $a\Lambda_1 = \Lambda_2$.

Théorème VI.4. Développement On note R l'ensemble des réseaux modulo isomorphismes. Alors l'application suivante est une bijection

$$\begin{array}{ccc} \mathcal{H}/SL_2(\mathbb{Z}) & \longrightarrow & R \\ \tau \mod SL_2(\mathbb{Z}) & \longmapsto & \mathbb{Z} \oplus \mathbb{Z}\tau \end{array}.$$

• VI.B Géodésiques de $\mathbb{H}$

[A completer]

VII Développements

- Action du groupe modulaire.
- $PSU_2(\mathbb{C}) = SO_3(\mathbb{R})$
- Automorphisme de $\mathbb{S}^2$.
- Étude des suites homographiques.
- Géodésiques de $\mathbb{H}$.

Exercice .1. Quelle est l'image de $\{Re \in [0,1]\}$ par $\dfrac{z-1}{z}$.

Démonstration. On a $\dfrac{z-1}{z} = 1 - \dfrac{1}{z}$. La droite $\{Re = 0\}$ est préservée $\dfrac{1}{z}$, et la droite $\{Re = 1\}$ est envoyé sur le cercle de diamètre $[0,1]$ par $\dfrac{1}{z}$. Puis on conclue en faisant une symétrie et une translation. □

Exercice .2. Soit $f : \mathbb{C} \to H^2$ holomorphe. Montrer que f est constante.

Démonstration. H^2 est biholomoprhe au disque D, donc on en déduit une application $\mathbb{C} \to D$. □

Exercice .3. Trouver un sous-groupe libre de $PSL_2(\mathbb{C})$ de rang 2, et un de rang 2 discret.

Démonstration. ... □

139 - Applications des nombres complexes à la géométrie

Références [Aud06], [Ber77], [Arniaudies 1].

Introduction La structure du corps des complexes est liée aux opérations affines du plan.

I Corps des complexes

• I.A Opérations sur les complexes

On identifie $\mathbb{C}$ à $\mathbb{R}^2$ via $(x,y) \mapsto z = x + iy$. On munie $\mathbb{C}$ de la norme eucidienne de $\mathbb{R}^2 |z|^2 = x^2 + y^2$ et de la conjugaison $\overline{z} = x - iy$.

II Exponentiel complexe

On définit l'exponentiel par $e^z = \sum_{n=0}^{+\infty} \frac{z^n}{n!}$.

$exp : \mathbb{C} \to \mathbb{C}^*$ est morphisme surjectif de noyau $2i\pi\mathbb{Z}$.

$exp : \mathbb{R}/2i\pi\mathbb{Z} \to \mathbb{U}$ est un isomoprhisme de groupe. Pour $z \in \mathbb{C}$ non nulle on appelle *argument* θ de z, l'antécédant de $z/|z|$.

Tout complexe non nulle a une forme polaire $z = re^{i\theta}$.

III Géométrie euclidienne plane

• III.A Propriétés géométriques

Proposition III.1. Soient $a, b, c, d \in \mathbb{C}$:
- La distance entre a et b est $|a - b|$.
- Le produit scalaire $\langle \overrightarrow{ab}, \overrightarrow{ac} \langle$ est $\mathrm{Re}(\overline{b-a})(c-a)$.
- L'angle $(\overrightarrow{ab}, \overrightarrow{ac})$ est $Arg(c-a)/(b-a)$.
- Les points a, b, c sont alignés si et seulement si $(c-a)/(b-a) \in \mathbb{R}$.
- Le triangle abc est équilatéral directe si et seulement si $a + jb + j^2 c = 0$.
- Les points a, b, c, d sont sur un cercle-droite si et seulement si $\frac{d-b}{d-a} / \frac{c-b}{c-a} \in \mathbb{R}$.

Applications III.2.
- Théorème de Napoléon : soit ABC un triangle, et PRQ les centres des triangles équilatéraux extérieurs à ABC. Alors PQR est un triangle équilatéral.
- Théorème de Morley : L'intersectection des trisectrices d'un triangle est un triangle équilatéral.
- Point de Fermat : le point F du plan qui minimise $AF + BF + CF$, vérifie $(FA, FB) = (FB, FC) = (FC, FA) = \frac{2\pi}{3}$.
- Droite de Steiner.

• III.B Similitudes de $\mathbb{R}^2 = \mathbb{C}$

Définition III.3. Une *similitude* de rapport $k > 0$ est une application qui multiplie les distances par k. Une similitude vectorielle est *orthogonal* si $k = 1$. Une similitude f est dite *directe* si $\det \overrightarrow{f} > 0$ et *indirecte* sinon.

Les similitudes de $\mathbb{C}$ sont de la forme :
- Translation : $z + t$.
- Rotation : $e^{it}(z - a) + a$.
- Homothétie : $\lambda(z - a) + a$, $\lambda \in \mathbb{R}^*$.
- Réflections : $e^{2it}\overline{z - a} + a$.

Applications III.4. ???

IV Géométrie projective dans $\mathbb{P}^1(\mathbb{C})$

• IV.A Droite projective complexe

Définition IV.1. La *droite projective complexe* est $\mathbb{P}^1(\mathbb{C}) = \mathbb{C}^2/\mathbb{C}^*$.

On injecte $\mathbb{C}$ dans $\mathbb{P}^1(\mathbb{C})$ via $z \mapsto [z : 1]$. On identifie alors $\mathbb{P}^1(\mathbb{C}) = \hat{\mathbb{C}}$.

• IV.B Homographies et inversions

Définition IV.2. Une *homographie* de $\mathbb{P}^1(\mathbb{C})$ est le quotient une application de $SL_2(\mathbb{C})$.

Toute application affine de $\mathbb{C}$ se prolonge en une unique homographie de $\mathbb{P}^1(\mathbb{C})$.

Définition IV.3. Une inversion de $\mathbb{C}$ de pôle $a \in \mathbb{C}$ et de rapport k est l'application :

$$\begin{array}{ccc} \mathbb{C} \setminus \{a\} & \longrightarrow & \mathbb{C} \setminus \{a\} \\ z & \longmapsto & \dfrac{k}{z-a} + a \end{array}.$$

Proposition IV.4. Les applications affines et l'inversion $1/z$ engendre l'ensemble des homographies.

• IV.C Birapport et cercles-droites

Proposition IV.5. Si (a, b, c) et (a', b', c') son des triplets de points distinct de $\mathbb{P}^1(\mathbb{C})$, alors il existe une unique homographie envoyant (a, b, c) sur (a', b', c').

Définition IV.6. Si (a, b, c) sont trois points distincts de $\mathbb{P}^1(\mathbb{C})$, alors l'homographie h envoyant (a, b, c) sur $(1, 0, \infty)$ définit un repère et pour $d \in \mathbb{P}^1(\mathbb{C})$, on note $[a, b, c, d] = h(d)$ le birapport de (a, b, c, d).

Proposition IV.7. Les homogrpahie préservent le birapport.

Définition IV.8. Une droite cercle est l'image de $\mathbb{P}^1(\mathbb{R})$ par une homographie. C'est aussi un ensemble C du type $E = \{d \in \mathbb{P}^1(\mathbb{C}) \mid [a, b, c, d] \in \mathbb{R}\}$ avec (a, b, c) distincts.

V Pavages du plan

[A compléter]

VI Tores complexes

• VI.A Réseaux de $\mathbb{C}$

Définition VI.1. Un réseau Λ est une sous-groupe discret de $\mathbb{C}$ de rang 2 : $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$. Un tore complexe est $\mathbb{C}$ quotienté par un réseau. Deux réseaux Λ, Λ' sont isomorphes si : $\exists z \in \mathbb{C}^*, z\Lambda = \Lambda'$.

Proposition VI.2. Soient $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ et $\Lambda' = \omega_1'\mathbb{Z} \oplus \omega_2'\mathbb{Z}$ deux réseau. Alors $\Lambda = \Lambda'$ ssi $\exists \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}$.

• VI.B Action du groupe modulaire

$SL_2(\mathbb{Z})$ agit sur $\mathcal{H}$ par homographie : pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\gamma.z = \dfrac{az+b}{cz+d}$.

Définition VI.3. Un réseau est un sous groupe discret de $\mathbb{C}$ de rang 2. Deux réseaux Λ, Λ' sont isomorphes s'il existe $c \in \mathbb{C}^*$ tel que $\Lambda = c\Lambda'$.

Théorème VI.4. L'application :

$$\begin{array}{ccc} \mathcal{H} & \longrightarrow & \{\text{Réseaux modulo isomorphisme}\} \\ \tau \mod SL_2(\mathbb{Z}) & \longmapsto & \mathbb{Z} \oplus \tau\mathbb{Z} \end{array}$$

est une bijection.

VII Corps des quaternions et géométrie affine

VIII Opérations sur les quaternions

[A compléter]

IX Action des quaternions sur $\mathbb{R}^3$

[A compléter]

X Intégrale sur un chemin

Applications X.1. [Théorème de Jordan] Développement Le complémentaire d'une courbe simple fermé admet deux composantes connexes.

XI Développements

- Corps des quaternions.
- Action du groupe modulaire.
- Théorème de Napoléon.
- Théorème de Jordan.

Exercice .1. Soien a, b, a, b' quatre points du plan. Existe-t-il un similitude qui envoie a sur a' et b sur b' ? Unicité ? Peut-on prendre un isométrie isométrie ?

Démonstration. Une similitude indirecte est de la forme $\alpha\bar{z} + \beta$. On veut alors :

$$\begin{cases} \alpha\bar{a} + \beta = a' \\ \alpha\bar{b} + \beta = b' \end{cases}$$

Si $a \neq b$ alors, $\det(\bar{a} - \bar{b}) \neq 0$, c'est à dire $a - b$ (si $a = b$, l'existence ou non est trivial). On alors $\alpha = (a' - b')/(\bar{a} - \bar{b})$. □

Exercice .2. Trouver les z tel que $Re\left((z-1)^2/(z-i)^2\right) = 0$.

Démonstration. On a $2Angle(z-1, z-i) = Arg\left((z-1)^2/(z-i)^2\right)$. Donc on cherche les z tel que $Angle(z-1, z-i) \in \mathbb{Z}\pi/4$. C'est alors des portion de cercles centrés aux points c_k tel que $Angle(c_k - 1, c_k - i) = k\pi/4$. □

140 - Systèmes d'équations linéaires. Systèmes échelonnés. Résolution. Exemples et applications.

Références [Arnaudies 1], [Escofier (alg. licence)].

I Généralités

II

III Développements

- Gradient conjugué.
- ? ? ?

141 - Utilisation des groupes en géométrie

Références [Aud06] [Ber77], [Tau97].

I Action du groupe orthogonal sur un espace euclien

On considère $\mathbb{R}^n$ munie de sa structure d'espace eucliden orienté. Le groupe $O_n(\mathbb{R})$ agit sur $\mathbb{R}^n$ en conservant le produit scalaire et le groupe $SO_n(\mathbb{R})$ agit en conservant le produit scalaire et le déterminant.

• I.A Notion d'angles dans $\mathbb{R}^2$ et $\mathbb{R}^3$

Définition I.1. Si u, v sont deux vecteurs unitaires de $\mathbb{R}^2$ alors il existe un unique $\theta \in \mathbb{R}/2\pi\mathbb{Z}$ tel que $R_\theta.u = v$. On appelle θ l'*angle orienté* entre u et v.

Définition I.2. Si D_1 et D_2 sont deux droites vectoriels, alors il existe deux $\theta \in \mathbb{R}/2\pi\mathbb{Z}$ tel que $R_\theta.D_1 = D_2$ et ses deux angles diffèrent de Π. On appelle θ mod π l'angle orienté endtre D_1 et D_2.

Proposition I.3. Soit $M \in SO_3(\mathbb{R})\backslash\{Id\}$. Alors M admet une unique droite stable D et M agit par rotation sur $D^\perp$. Le choix d'une orientation de D induit une orientation sur $D^\perp$ et on appelle angle de M l'angle de $M_{|D^\perp}$ (dépendant au signe près du choix de l'orientation de D).

• I.B Structure du groupe orthogonal

Proposition I.4 (Structure des isométries)**.** Tout éléments de $O_n(\mathbb{R})$ est conjugué à $diag(1, \dots, -1, \dots, R_{\theta_1})$, avec $R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$.

Théorème I.5. Le groupe $O_n(\mathbb{R})$ est un groupe compact.

Le groupe $GL_n(\mathbb{R})$ agit sur des produits scalires de $\mathbb{R}^n$.

Théorème I.6. Développement Si G est un sous-groupe compact de $GL_n(\mathbb{R})$, alors G préserve un produit scalaire.

• I.C Polytopes et sous-groupes finis de $SO_n(\mathbb{R})$ pour $n = 2, 3$

Proposition I.7. Les sous-groupes finis de $O_2(\mathbb{R})$ sont : $\mathbb{Z}/n\mathbb{Z}$ $(n \in \mathbb{N})$ et $D_{2n} = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ $(n \in \mathbb{N})$.

Exemple I.8.
- $\mathbb{Z}/n\mathbb{Z}$ est le groupe engendré par une rotation d'ordre n.
- $D_{2n} = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est le groupe des isométrie d'un n-gone.

Définition I.9. Un *polyèdre* est l'enveloppement convexe d'un nombre fini de points non coplanaires. Un polyèdre est *régulier* si toutes ses faces ont des polygônes réguliers isométriques et si chaque sommets a un même nombre d'arrêtes.

Théorème I.10.
- Le groupe des isométries du tétraèdre est isomorphe à $\mathfrak{A}_4$.
- Le groupe des isométries du cube est isomorphe à $\mathfrak{S}_4$.
- Développement Le groupe des isométries du dodécaèdre est isomorphe à $\mathfrak{A}_5$.

Théorème I.11. Développement Les sous-groupes finis de $SO_3(\mathbb{R})$: sont isomorphes à : $\mathbb{Z}/n\mathbb{Z}/$, D_{2n}, $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$. De plus si deux sous-groupes sont isomorphes, alors ils sont conjugués.

Exemple I.12.
- $\mathbb{Z}/n\mathbb{Z}$ est le groupe engendré par une rotation d'ordre n.
- D_{2n} est le groupe des déplacements d'un prisme de base un n-gone.

II Géométrie affine

• II.A Généralités

Définition II.1.
- Un *espace affine* de direction E est un ensemble $\mathcal{E}$ munie d'une action par E simplement transitive.
- Une *application affine* entre deux espaces affines $\mathcal{E}$ et $\mathcal{F}$ est une application f telle qu'il existe une application ϕ linéaire entre E et F compatible avec les actions sur $\mathcal{E}$ et $\mathcal{F}$. On note $GA(\mathcal{E})$ les bijections affines de E.

L'ensemble des translations forment un groupe isomorphe canoniquement à E.

Proposition II.2. Si on fixe un point O de $\mathcal{E}$, alors on a une bijection cononique $GA(\mathcal{E}) \cong E \rtimes GL(E)$.

Si E est un espace euclidien, alors $\mathcal{E}$ hérite d'une métrique euclidienne. Une application affine conservant les distances est une *isométries*.

Proposition II.3. Une application affine est une isométrie si et seulement si $\vec{f}$ est une isométrie.

• II.B Représentation par les complexes et les quaternions

Corps des complexes On identifie le plan $\mathbb{R}^2$ à $\mathbb{C}$.

Proposition II.4. La multiplication par $z = x + iy$ a pour matrice $\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$.

Proposition II.5. Les similitudes directes sont de la forme $z \mapsto az+b$ avec $a, b \in \mathbb{C}$ et $a \neq 0$. Les similitudes indirectes sont de la forme $z \mapsto a\bar{z} + b$.

Proposition II.6. Soient $a, b, c \in \mathbb{C}$. Alors abc forment un triangle équilatéral direct si et seulement si $a + bj + cj^2 = 0$.

Applications II.7.
- Théorème de Napoléon : soit ABC un triangle, et PRQ les centres des triangles équilatéraux extérieurs à ABC. Alors PQR est un triangle équilatéral.
- Théorème de Morley : L'intersectection des trisectrices d'un triangle est un triangle équilatéral.

Corps des quaternions Soit E un espace euclidien orienté. Le corps des quaternions est $\mathbb{R} \oplus E$, muni la multiplication $(x+\vec{u}).(y+\vec{v}) = xy - \vec{u}.\vec{v} + x\vec{u} + y\vec{v} + \vec{u} \wedge \vec{v}$. On le note $\mathbb{H}$. On munie aussi $\mathbb{H}$ de la norme euclidienne et de la conjugaison $\overline{(x+u)} = x - u$. On note U l'ensemble des quaternions de norme 1. On appelle E l'espace des quaternions purs.

Proposition II.8 (Structure des quaternions)**.**
- $\mathbb{H}$ est un corps non commutatif dont le centre est $\mathbb{R}$.
- La norme est multiplicative.
- Tout quaternion non nul s'écrit de façon unique sous la forme rn avec $r \in \mathbb{R}_+$ et $n \in U$.
- La multiplication par $q \in U$ est un élément de $SO(\mathbb{H})$.

Proposition II.9. Developpement Alors on a un isomophisme $U/\{\pm 1\} \cong SO(E)$. Si $q = \cos\theta + \sin\theta u$ est un quaternion unitaire alors la conjugaison par q est la rotation d'angle 2θ autour de u.

Corollaire II.10. Les automorphismes de corps de $\mathbb{H}$ sont tous intérieurs.

Proposition II.11. On a un isomophisme $U \times U/\{\pm(1,1)\} \cong SO(\mathbb{H})$.

• II.C Pavages du plan

Définition II.12. Un pavage du plan euclidien E est un couple (P, G) où P est un compact d'intérieur non vide de E et G un sous-groupe de $Isom^+(E)$ vérifiant :
- $E = \bigcup_{g \in G} g(P)$.
- Pour tout $g, h \in G$, si $int(g(P)) \cap int(h(P)) \neq \emptyset$, alors $g(P) = h(P)$.

Théorème II.13. Développement Il existe 5 types de pavages directs du plan et 12 non-directs.

Exemple II.14. ???

III Groupe libre et théorème de Banach-Tarski

• III.A Structure du groupe libre de rang 2

Définition III.1. Le *groupe libre* de rang 2, noté F_2, est l'ensemble des mots sur $\{a, a^{-1}, b, b^{-1}\}$, munie de la concaténation avec ε le mot vide et la règle $aa^{-1} = a^{-1}a = bb^{-1} = b^{-1}b = \varepsilon$.

Tout éléments de F_2 s'écrit de façon unique sous la forme $a^{\alpha_1}b^{\beta_1}\dots a^{\alpha_p}b^{\beta_p}$, avec $\alpha_i, \beta_i \in \mathbb{Z}^*$ et $\alpha_1, \beta_p \in \mathbb{Z}$.

• III.B Duplication de la sphère

Théorème III.2. Développement [Banach-Tarski faible] Il existe :
- D une partie dénombrable au plus de $\mathbb{S}^2$.
- Une partition de $\mathbb{S} \setminus D$ en 4 partie : $\mathbb{S} \setminus D = A_1 \sqcup A_2 \sqcup A_3 \sqcup A_4$
- Deux rotations $f, g \in SO_3(\mathbb{R})$.

Tels que

$$\mathbb{S}^2 \setminus D = A_1 \sqcup a(A_2) = A_3 \sqcup b(A_4).$$

(On admettra que $\mathbb{Q} \cap \cos(\mathbb{Q}\pi) = \{\pm 1, \pm 2^{-1}, 0\}$).

IV Action du groupe modulaire sur le demi-plan de Poincarré

• IV.A Définitions

Le demi-plan de Poincaré est $\mathcal{H} = \left\{ z \in \mathbb{C} \mid \operatorname{Im} z > 0 \right\}$. Le *groupe modulaire* $SL_2(\mathbb{Z})$ agit sur $\mathcal{H}$ par homographie : pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ et $z \in \mathcal{H}$, l'action de γ sur z est : $\gamma.z = \dfrac{az+b}{cz+d}$.

On note $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Les actions de ces matrices sur z sont alors : $S.z = \dfrac{-1}{z}$ et $T.z = z + 1$.

Proposition IV.1. Le groupe modulaire est engendré par S, T.

• IV.B Domaine fondamentale et classification des réseau de $\mathbb{C}$

Proposition IV.2. Un domaine fondamental pour cette action est $\{z \in \mathcal{H} \mid |Re(z)| \leq 1, |z| \geq 1\}$.

Théorème IV.3. Développement Les orbites de $SL_2(\mathbb{Z})$ sur $\mathcal{H}$ sont en bijection avec les tores complexes.

V Développements

- Théorème de Banach-Tarski.
- Sous-groupe compact de $GL_n(\mathbb{R})$.
- Sous-groupes finis de $O_2(\mathbb{R})$ et de $SO_2(\mathbb{R})$.
- Pavages du plan.
- Corps des quaternions.
- Action du groupe modulaire.
- Colorigage du cube.

VI Exercice

Exercice .1. Trouver le groupe des applications affine préservant un parallélogramme.

Exercice .2. On se donne un ellipse. Trouver les triangles inscrit d'aire maxiamle.

Exercice .3. Soit G sous-groupe discret des isométries affines positives d'un plan affine. On suppose que G préserve un compact. Montrer que G est cyclique.

Démonstration. Soit K compact préservé par G. Le sous-groupe des translations de G est réduit au neutre car sinon K ne pourrait pas être stable. Le commutateur de deux éléments est est une translations donc G est abélien. Donc toute les rotations de G ont le même centre. Comme G est discret, c'est un groupe monogène de $SO_2(\mathbb{R})$. □

144 - Problèmes d'angles et de distances en dimension 2 ou 3

Références [...]

I Géométrie euclidienne en dimension 2 et 3

• I.A Structure des espaces eucldiens

Définition I.1. distance...

Définition I.2. Angle...

[A completer]

• I.B Groupe des isométries et des similitudes

Définition I.3. Isométries, directes, indirectes...

[A completer]

• I.C Différentielle de la distance

Théorème I.4. Gradient de la norme ...

Applications I.5. Propriétés focales des côniques...

Théorème I.6. Développement Différentiabilité de la fonction distance...

Théorème I.7 (Motzkin)**.** ...

II Géométrie plane

• II.A Relations métriques et trigonométriques dans un triangle

Théorème II.1 (Pythagore)**.** Si ABC est un triangle droit en A, alors $AB^2+AC^2 = BC^2$.

Théorème II.2 (Thalès)**.** ...

Proposition II.3. Relations dans un triangle...

• II.B Théorème de l'angle inscrit

Théorème II.4 (Angle inscrit)**.** ...

• II.C Applications conformes de $\mathbb{C}$

Définition II.5. Une application conforme est une application $f : \mathbb{C} \to \mathbb{C}$, C^1 du plan tel que pour tout couple de chemins (γ_1, γ_2) passant par un point M, on ait

$$(\gamma_1'(0), \gamma_2'(0)) = ((f \circ \gamma_1)'(0), (f \circ \gamma_2)'(0)).$$

.

Proposition II.6. Les applications conformes sont les applications holomorphes dont la dérivée est non nulle.

• II.D Nombres constructibles

Définition II.7. Soit Σ une partie de $\mathbb{C}$. Un nombre $z \in \mathbb{C}$ est dit *construtible* à la règle et au compas à partir de Σ si il existe une suite $P_1, \dots, P_n$ telle que

- $z = P_n$.
- Pour tout $i \leq n$, P_i est intersection de droites passant par deux points de $\Sigma_{i-1} := \Sigma \cup \{P_1, \dots, P_{i-1}\}$ ou de cercles centré en un point de Σ_{i-1} passant par un point Σ_{i-1}.

On note C_Σ leur ensemble.

Théorème II.8 (Mohr-Mascheroni)**.** Tout point constructible à règle et au compas est constructible au compas seul.

Démonstration. .[A completer] □

Théorème II.9 (Wantzel, 1837)**.** Soit E un sous-corps de R. Un complexe z est constructible à partir de E si et seulement s'il existe une suite de sous-corps de $\mathbb{C}$

$$E = E_0 \subset E_1 \subset \cdots \subset E_n$$

tels que

- $x \in E_n$.
- $\forall i \in [i, n], [E_i : E_{i-1}] = 2$.

Conséquences :

- Un nombre constructible est de degré une puissance de 2 sur le corps de départ.
- $\sqrt[3]{2}$ n'est pas constructible sur $\mathbb{Q}$.
- L'angle $\alpha/3$ est constructible si et seulement si $X^3 - 3X + 2\cos(\alpha)$ n'est pas irréductible sur $\mathbb{Q}$.

Remarque II.10. La réciproque est fausse : les racines de $X^4 - X - 1$ ne sont pas constructibles.

III Côniques

• III.A Définitions focales des côniques

[A completer]

• III.B Propriétés

[A completer]

IV Développements

- Différentiabilité de la disance.
- Point de Fermat.
- Théorème Wantzel.

145 - Méthodes combinatoires, problèmes de dénombrement.

Références [...]

I Calcul de cardinaux

• I.A Cardinal des ensembles

Définition I.1. Un ensemble X est de cardinal fini n s'il est en bijection avec $[1, n]$. Auquel cas n est unique. Sinon il est de cardinal infini.

Proposition I.2. Soient E et F deux ensembles.
- Si E et F sont en bijection alors ils ont le même cardinal.
- Si $E \subset F$, alors $\operatorname{Card} E \leq \operatorname{Card} F$.
- Si E et F on même cardinal fini et si $E \subset F$, alors $E = F$.

Exemple I.3.
- Les carrés de $\mathbb{F}_p$ sont exactement les racines de $X^{(p-1)/2} - 1$.
- ? ? ?

• I.B Théorèmes de dénombrement

Théorème I.4 (Principe des tiroirs de Dirichlet)**.** Si $\operatorname{Card} E > \operatorname{Card} F$, alors il n'existe pas d'injections de E dans F.

Exemple I.5. ? ? ?.

Théorème I.6 (Principe des Berger)**.** Si X se partitionne en p sous-ensemble de cardinal n, alors $\sharp X = pn$.

Exemple I.7. Théorème de Lagrange : si H est un sous-groupe de G fini, alors $\sharp H | \sharp G$.

Théorème I.8 (Formule de la crible)**.** Si $(A_i)_{i\in\mathbb{N}}$ est une famille finie de sous-parties de X, alors $\sharp \bigcup_{i\in[1,n]} A_i = \sum_{J\subset I} (-1)^{|J|+1} \operatorname{Card} \bigcap_{i\in j} A_j$.

Exemple I.9.
- Dénombrement de permutations sans points fixes.
- Dénombrement du nombre de surjections E dans F.

Théorème I.10 (Double comptage)**.** ...

Exemple I.11. Formule d'Euler : $S - A + F = 2$.

• I.C Ensemble des applications et ensemble des parties

Proposition I.12.
- Soient E et F de cardinal finis. Alors le nombre d'applications de E dans F est $\operatorname{Card} F^{\operatorname{Card} E}$.
- L'ensemble des bijections de E, est de cardinal $\operatorname{Card} E!$.

Exemple I.13. Probabilité d'avoir 4 as dasn une main de 5 cartes.

Proposition I.14.
- Le nombre de parties à k éléments dans un ensemble de cardinal n est : $\binom{n}{k} = \frac{n!}{—}$.
- Si $k_1 + \cdots + k_p = n$, alors le nombre partitions en p parties de $k_1, \ldots, k_p$ éléments est : $\dfrac{n!}{k_1! \ldots k_p!}$.
- Triangle de Pascal : $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Exemple I.15.
- Formule du binôme : $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.
- Loi binomiale : la probabilité de réussite de k Bernoulli de paramètre p parmi n, est $\binom{n}{k} p^k p^{n-k}$
- ? ? ?

Proposition I.16. On a $\operatorname{Card}(P(E)) = 2^{\operatorname{Card} E}$.

II Utilisation de fonctions et de séries génératrices

• II.A Produit de convolution et fonction de Mobius

Définition II.1. produit de convolution.

Définition II.2. Indicatrice d'Euler. Fonction de Mobius.

Exemple II.3.
- Polynômes irreductibles de $\mathbb{F}_q$.
- Développement Probabilité pour que deux nombres soient premiers entre eux.

• II.B Séries génératrices

Définition II.4. Produit de Cauchy. Séries génératrices.

Exemple II.5.
- $\dim K_d[X_1, \ldots, X_n] = \binom{n+d-1}{d-1}$.
- Dénombrement des partitions de $[1, n]$.
- Développement Dénombrement des solutions de $a_1 n_1 + \cdots + a_p n_p = n$.

III Utilisation à la théorie des groupes

Définition III.1. Soit G un groupe et X un ensemble. Une *action* de G sur X est un morphisme de groupe $G \to Bij(X)$. L'action de $g \in G$ sur $x \in X$ sera noté $g.x$.

Proposition III.2. Pour tout $x \in X$, on a $\sharp Orb_G(x).\sharp Stab_G(x) = \sharp G$.

Théorème III.3. Si $(x_1, \ldots, x_p)$ est un système de représentant des orbites, alors $\sharp X = \sum_{i=1}^{p} \sharp Orb_G(x_i)$.

Applications III.4. L'action par conjugaison donne l'équation des classes

$$\sharp G = Z(G) + \sum_{Cl(x_i) \neq Cl(1)} \sharp Orb_G(x_i).$$

Donc le centre d'un p-groupe est non trivial.

Corollaire III.5. Si g est un p-groupe, alors $\sharp \bigcap_{g \in G} Fix(g) = \sharp X \mod p$.

Applications III.6. Développement Théorème de Wedderburn : tout corps fini est commutatif.

Théorème III.7 (Formule de Burnside)**.** $\sharp G \sharp Orbites = \sum_{g \in G} \sharp Fix_X(g)$.

Applications III.8. Développements Dénombrement des coliers de perles et dénombrement des coloriages du cube.

Théorème III.9 (Sylow)**.** ...

Théorème III.10. Développement [Sylow] Tout groupe fini admet un p-Sylow. De plus tous les p-Sylow sont conjugués et le nombre de p-Sylw est congrue à 1 $\mod p$ et divive $\sharp G$.

Applications III.11. L'action de G sur ses Sylows permet de démontrer les choses suivantes

- Tout sous-groupe d'ordre < 60 n'est pas simple ou est trivialement simple.
- Développement Le groupe $\mathfrak{A}_5$ est le seul sous-groupe d'ordre 60.

IV Développements

- Denombrement d'une équation diophantienne.
- Probabilité pour que deux nombres soient premiers entres eux.
- Theoreme de l'amitie.
- Sous-groupes finis de $SO_3(\mathbb{R})$.
- Polynômes irréductibles de $\mathbb{F}_p$.
- Théorème de Sylow.
- Théorème de Kronecker.
- Coloriage du cube.

• IV.A Exercice

Exercice .1 (Agreg 2010)**.** Dénombrer le nombre d'orbites de l'action $GL_n(\mathbb{R})$ sur $S_n(\mathbb{R})$ par conjugaison.

146 - Résultant de deux polynômes, applications à l'intersection de courbes ou de surfaces algébriques.

Références [...]

Introduction

Définition et propriétés

Soit $\mathbb{A}$ un anneau factoriel. On se donne $p, q \in \mathbb{N}$ deux entiers et $P(X) = a_pX^p + \cdots + a_0 \in A[X]_p$ et $Q(X) = b_qX^q + b_{q-1}X^{q-1} + \cdots + b_0 \in A[X]_q$. On note $f_{P,Q}$, l'application :

$$\begin{array}{rccc} f_{P,Q} : & A[X]_{q-1} \times A[X]_{p-1} \cong A[X]_{p+q-1} & \longrightarrow & A[X]_{p+q-1} \\ & (U, V) \cong UX^p + V & \longmapsto & UP + VQ \end{array}.$$

La *matrice de Silvester* de (P, Q) est la matrice de f dans la base :

$$(X^{q-1}, X^{q-2}, \ldots, 1, X^{p-1}, X^{p-2}, \ldots, 1)$$

de $A[X]_{q-1} \times A[X]_{p-1}$ et la base

$$(X^{p+q-1}, \ldots, X, 1)$$

de $A[X]_{p+q-1}$. Le résultant de (P, Q), noté $Res(P, Q)$ est le déterminant de cette matrice.

Remarque .1. Le résultant de P, Q dépend de P et de Q, mais aussi de p, q ! ! !

Proposition .2.
- Si $\deg P < p$ et $\deg Q < q$, alors $Res(P, Q) = 0$.
- Si $\deg Q \leq q - 1$, alors $Res_{p,q}(P, Q) = a_p Res_{p,q-1}(P, Q)$.

Théorème .3. On suppose que A est intègre. Si $\deg P = p$ ou $\deg Q = q$, alors $Res(P, Q) = 0$ si et seulement si $pgcd(P, Q) \neq 1$.

Proposition .4. On suppose que $a_p \in A^\times$. Si m_Q est la multiplication apr Q dans $k[X]/P$, alors $Res(P, Q) = a_p^q \det m_Q$.

I Règles de calcul

Proposition I.1. On prend P, Q quelconques.
- $Res(P, Q) = (-1)^{pq} Res(Q, P)$.
- $Res(aP, bQ) = a^q b^p Res(Q, P)$.
- Si $a_p \in A^\times$ et si $Q = AP + R$, alors $Res(P, Q) = Res(P, R) a_p^{\deg Q - \deg R}$.
- $Res(X - a, P) = P(a)$.
- $Res(P(X - a), Q(X - a)) = Res(P, Q)$.
- $Res(P, QR) = Res(P, Q) Res(P, R)$.

Applications I.2. Développement [Loi de réciprocité quadratique] ...

Spécialisation

I Résultant universel

Définition I.1. On note $P_u = A_pX^p + ... + A_0 \in \mathbb{Z}[\overrightarrow{A}, \overrightarrow{B}, X]$ et $Q_u = B_qX^q + ... + B_0 \in \mathbb{Z}[\overrightarrow{A}, \overrightarrow{B}, X]$ les polynômes universels. Le résultant universel $Res(P_u, Q_u)$ est alors un polynôme dans $\mathbb{Z}[\overrightarrow{A}, \overrightarrow{B}]$.

[A completer]

II Expression en fonctions des racines

Théorème II.1. Si $P = \prod_{i=1}^{p}(X - R_i)$ et $Q = \prod_{j=1}^{q}(X - S_j)$, alors

$$Res(P, Q) = \prod_{i,j}(S_j - R_i) = \prod_{j=1}^{q} P(S_j) = (-1)^{pq} \prod_{j=i}^{p} Q(R_i).$$

Corollaire II.2. Si $P(X)$ et $Q(X)$ ne sont plus unitaires alors

$$Res(P, Q) = b_q^p \prod_{y \in Q^{-1}(0)} P(y) = a_p^q (-1)^{pq} \prod_{x \in P^{-1}(0)} Q(x).$$

III Discriminant

Proposition III.1. Soit $P \in A[X]$. Alors

$$P(X) \text{ a une racine double} \iff pgcd(P, P') \neq 1 \iff Res(P, P') = 0.$$

Définition III.2. Si P est un polynôme de degré p, alors son *discriminant* est :

$$disc(P) = a_p^{2p-2} \prod_{\{y,z\}} (y - z)^2,$$

où $\{y, z\}$ parcourt les paires de racines de P.

Exemple III.3.
- Le discriminant de $aX^2 + bX + C = aX^2 - a(r_1 + r_2)X + ar_1r_2$ est $\Delta = b^2 - 4ac$.
- Le discriminant de $X^3 + pX + q$ est $\Delta = -4p^3 - 27q^2 = -2^2p^3 - 3^3q^2$.

Remarque III.4. Si $P(X)$ est de degré 1 alors son discriminant est 1.

Proposition III.5. On a $Res(P, P') = a_p(-1)^{p(p-1)/2} disc(P)$.

Théorème III.6. Le discriminant $disc(P)$ est un polynôme homogène de degré $2p - 2$ en les coefficients de $P(X)$.

Élimination

On se place dans un corps.

I Théorème fondamentale

Théorème I.1. Soient $P, Q \in K[\overrightarrow{A}, X]$, alors $Res_X(P,Q)$ annule $a_1, \ldots, a_n$ si et seulement si $\exists x \in \overline{K}, P(\overrightarrow{a}, x) = 0$ et $Q(\overrightarrow{a}, x) = 0$.

Exemple I.2. Si a et b sont deux nombres algébrique de polynômes annulateurs $P(X)$ et $Q(X)$ sur un corps K, alors $Res_T(P(T), Q(X-T))$ est un polynôme annulateur de $a+b$, et $Res_T(P(T), Q(X/T)T^q)$ est un polynôme annulateur de xy.

II Intersection de courbes

On suppose que k est clos.

Définition II.1. Si I est un idéal de $k[X_1, \ldots, X_n]$, on note $V(I) = \{x \in k^n : \forall P \in IP(x) = 0\}$.

Soient $P(X,Y), Q(X,Y) \in k[X,Y]$. On note V_x la projection de $V(P,Q)$ sur la première composante. Alors V_x est inclus dans les racines de $Res_Y(P(X,Y), Q(X,Y))$ et V_y inclus dans les racines de $Res_X(P(X,Y), Q(X,Y))$.

Plus généralement si $P(X_1, X_2, \ldots, X_n), Q(X_1, X_2, \ldots, X_n)$ sont deux polynômes, alors la projection de $V(P,Q)$ sur les $n-1$ premières composantes est donnée par l'équation $Res_{X_n}(P,Q) = 0$.

Soient $P(X,Y,Z), Q(X,Y,Z), R(X,Y,Z) \in k[X,Y,Z]$ sont 3 polynômes en 3 variables. Pour chercher $V(P,Q,R)$, on calcule le résultant $Res_Z(P,Q)$ donne la projection de $V(P,Q)$ et $Res_Z(P,R)$ donne la projection de $V(P,R)$. La projection de $V(P,Q,R)$ est alors incluse dans $V(Res_Z(P,Q)) \cap V(Res_Z(P,R)) = V(Res_Z(P,Q), Res_Z(P,R))$. La projection de $V(P,Q,R)$ sur la première composante est inclus dans la variété définie par : $Res_Y\Big(Res_Z(P,Q), Res_Z(P,R)\Big)$.

Théorème II.2. Développement [Bezout faible] deux courbes algébrques projectives de degré p et q sans composantes commune s'intersectent en au plus pq points.

III Équations de courbe de courbe paramétrée

Théorème III.1. Soient $P(T), Q(T) \in k[X]$. Alors $Res_T(X - P(T), Y - Q(T))$ est une équation cartésienne de la courbe paramétré $t \mapsto (P(t), Q(t))$ dans $\overline{k}$.

IV Développements

- Théorème de Bezout.
- Loi de réciporcité quadratique.

148 - Formes quadratiques réelles. Exemples et applications

Références [Berger 4], [Arnaudies 3], [Tauvel], [Goblot], [Perrin], [Escofier (alg. licence)].

I Généralités sur les formes quadratiques

• I.A Définitions

Définition I.1. Soit E un $\mathbb{R}$-espace vectoriel.
- Une *forme bilinéaire* sur E est une application $f : E \times E \to k$ linéaire en chaque variable.
- Elle symétrique si : $\forall x, y \in E, f(x,y) = f(y,x)$. Sa forme quadratique est $q(x) = f(x,x)$ et f est la forme polaire de q.
- Une forme quadratique q est non dégénérée si $\forall x \in E, (\forall y \in E, f(x,y) = 0) \Longrightarrow x = 0$.

On note $Q(E)$ l'ensemble des formes quadratiques sur E.

Définition I.2.
- Deux vecteurs (x,y)sont *q-orthognonaux* si $f(x,y) = 0$.
- Si F est un sous-espace, alors son orthogonal est
$$F^\perp = \{x \in E : \forall y \in F, f(x,y) = 0\} = \bigcap_{y \in F} \ker f(.,y).$$

Exemple I.3.
- La covarianve
-

Proposition I.4. Soit q une forme quadratique de forme polaire f.
- $\forall x, y \in E \forall \lambda \in k, q(x+y) = q(x) + 2f(x,y) + q(y)$ et $q(\lambda x) = \lambda^2 x$.
- Formule de polarisation :
$\forall x, y \in E, f(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)) = \frac{1}{4}(q(x+y) - q(x-y))$.
Donc si $q = 0$
- Soit $p : E \to k$, alors p est une forme quadratique si et seulement si : $\forall x \in E, \forall \lambda \in k, p(\lambda x) = \lambda x^2$ et $(x,y) \mapsto \dfrac{1}{2}(q(x+y) - q(x) - q(y))$ est bilinéaires.
- Pythagore : si x et y sont orthogonaux, alors $q(x) + q(y) = q(x+y)$.

Exemple I.5.
- Sur $\mathbb{R}^n$ les formes quadratiques sont les polynômes homogènes de degré 2.
- Sur l'ensemble des variables aléatoires L^2 sur $\mathbb{R}$, la variance est une forme quadratique. Si deux v.a. sont indéprendants alors $Var(X+Y) = Var(X) + V(Y)$.
- ? ? ?

• I.B Représentation matricielle et dualité

On se place ici en dimension finie. On rappelle que pour $f \in L(E,F)$, son application duale ${}^t f \in L(F^*, E^*)$ est définie par $\forall \phi \in F^*, \forall x \in E, {}^t f.\phi.x = \phi.f.x$. Si $x \in E$, sa transposée est ${}^t x : \phi \mapsto \phi.x \in L(E^*, \mathbb{R})$.

Définition I.6.
- Pour f une FBS, on lui associe l'application
$Q : \begin{array}{ccc} E & \longrightarrow & E^* \\ x & \longmapsto & f(.,x) \end{array}$. Le fait que f est symétrique signifie que ${}^t Q = Q$.
- Le *noyau* de f est noyau de Q : $\ker Q = \{x \in E : \forall y \in E, f(y,x) = 0\}$.

On peut alors écrire : $\forall x \in E, q(x) = {}^x.Q.x$.

Définition I.7. Soit $(e_i)_{i \in [1,n]}$ une base de E. La matrice de f est la matrice de Q dans les bases $(e_i)_{i \in [1,n]}$ et $(e_i)_{i \in [1,n]}$.

On a $Mat_e(f) = Mat_e^{e^*}(u) = [f(e_i, e_j)]_{i,j \in [1,n]}$.

• I.C Endomorphismes orthogonaux

[A completer]

II Réduction des formes quadratiques en dimension finie

III Orthogonalité

Proposition III.1. Si q est non dégénérée, alors $\dim F = codim\ F$. Si de plus F n'a pas de vecteurs isotropes alors $F \oplus F^\perp = E$.

• III.A Théorème de Sylvester et signature

Théorème III.2 (Sylvester)**.** Tout forme quadratique admet une base de vecteurs orthogonaux. De façon équivalente : il existe une base $(\phi_i)_{i \in [1,n]}$ de E^*, et des scalaires $(\lambda_i)_{i \in [1,n]}$ tels que $q = \sum_{i=1}^n \lambda_i \phi_i^2$.

Applications III.3. Algorithme de réduction : [A completer]

Théorème III.4 (Classification)**.** Il existe une base dans laquelle f a pour matrice $diag(I_p, -I_q, 0)$. De plus le couple (p,q) est unique et caractérise la classe de congruence de f.

Remarque III.5. Le rang de f est $p+q$.

Définition III.6. Le couple (p,q) est la *signature* de f.

Exemple III.7. ? ? ?

Applications III.8. ? ? ?

IV Espaces préhilbertiens

• IV.A Produits scalaires

Définition IV.1. Un *produit sclaire* est une forme bilinéaire $\langle .,. \rangle$ symétrique définie positive, c'est-à-dire : $\forall x \in E - \{0\}, \langle x, x \rangle > 0$. On note $\|.\|$ sa forme quadratique.

Proposition IV.2.
- Cauchy-Schsartz : $\forall x, y \in E, |\langle x, y \rangle| \leq \|x\|.\|y\|$ avec égalité si et seulement si x et y sont liés.
- Minkovski : $\forall x, y \in E, \|x + y\| \leq \|x\| + \|y\|$ avec égalité si et seulement si x et y sont positivement liés.

Corollaire IV.3. La forme quadratique $\|.\|$ définit une norme sur E.

Exemple IV.4.
- Sur $\mathbb{R}^n$: $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$.
- Sur $\mathbb{R}[X]_n$: $\langle P, Q \rangle = \int_0^1 P(x)Q(x)dx$.

Définition IV.5. Un espace *euclidien* est un $\mathbb{R}$-espace vectoriel normé muni d'un produit scalaire.

Proposition IV.6. Dans un espace euclidien
- $F \oplus F^\perp = E$ pour tout sous-espace F.
- ???

• IV.B Bases orthonormées

Soit E un espace eucidien de dimension n.

Proposition IV.7. Toute famille orthogonale de vecteurs non nul est libre.

Théorème IV.8 (Orthogonalisation de Gram-Schmidt)**.** Soit $(e_i)_{i \in [1,n]}$ une base de E. Alors il existe une unique base orthogonal $(f_i)_{i \in [1,n]}$ tel que : $\forall i \in [1, n], vect(e_1, \ldots, e_i) = vect(f_1, \ldots, f_i)$, et $e_i - f_i \in vect(e_1, \ldots, e_i)$. De plus cette famille est donnée par les formules de Gram-Schmidt : $f_i = e_i - \sum_{k=1}^i \frac{\langle e_k, f_i \rangle}{\|f_k\|^2} f_k$.

Applications IV.9.
- Tout espace euclidien de dimension n est isomorphe à $(\mathbb{R}^n, \|.\|_2)$: si $(e_i)_{i \in [1,n]}$ est une base
- ???

V Applications

• V.A Quadriques

On note $E = \mathbb{R}^n$ (en tant qu'espace vectoriel) et $\bar{E} = P(\mathbb{R} \times \mathbb{R}) = P^n(\mathbb{R})$ sa complétion projective.

Définition V.1.
- Un polynôme de degré 2, noté P, sur E est une fonction polynomiale de $\mathbb{R}[X_1, \ldots, X_n]$ sur $E = \mathbb{R}^n$ de degré total 2 au plus.
- On note d sa partie homogène de degré 2, et Q la complétion projective de P définei par $\begin{array}{rccc} Q : & \mathbb{R}^{n+1} & \longrightarrow & \mathbb{R} \\ & (x,t) & \longmapsto & t^2 P(x/t) \end{array}$.
- La *quadrique associé* à P est l'ensemble de ses zéros.
- La quadrique est dite non dégénérée si Q est est non dégénéré.

Exemple V.2.
- ???
- ???

Le groupe affine $GA(E) \times \mathbb{R}^*$ agit sur l'ensemble des polynômes de degré 2 sur E par : $(L, t).P = tP \circ L^{-1}$.

Proposition V.3 (Classification)**.** On note (p, q) la signature de d et (p', q') la signature de Q. Alors deux polynômes sont dans la même orbite si et seulement si (p, q, p, q') sont les même au signe près. Un système de représentants est donnés
- Si $(p', q') = (p, q)$, alors $P \simeq x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$.
- Si $(p', q') = (p + 1, q)$, alors $P \simeq x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2 + 1$.
- Si $(p', q') = (p, q + 1)$, alors $P \simeq x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2 - 1$.
- Si $(p', q') = (p+1, q+1)$, alors $P \simeq x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2 + x_{p+q+1}$.

• V.B Hessienne d'une fonction

Proposition V.4 (Schwartz)**.** Soit E un espace vectoriel de dimension finie. Si $f : E \to \mathbb{R}$ est une fonction C^2, alors pour tout $x \in E$ la fonction $D^2 f(x) \in L(L(E), E) \simeq Bil(E \times E, \mathbb{R})$ est symétrique.

Définition V.5. La Hessienne de f au point x, noté $Hf(x)$ est la forme quadratique associé à $D^2 f(x)$.

Proposition V.6 (Formule de Taylor)**.** On a $f(x+h) = f(x) + Df(x).h + \int_0^1 (1-t)^h . D^2 f(x+th).hdt = f(x) + Df(x).h + \int_0^1 (1-t) Hf(x)(h)dt$.

Théorème V.7 (Lemme de Morse)**.** Soit $f : E \to \mathbb{R}$ une fonction C^k avec $k \geq 3$ telle que $f(0) = 0$, $Df(0) = 0$ et $D^2 f(0)$ est une forme quadratique non dégénérée. Alors il existe $\Phi : U \to V$, un C^{k-2}-difféomorphisme entre deux voisinages de 0 tel que $D\phi(0) = Id$ et $:\forall x \in U, f(x) = \frac{1}{2} Hf(0)[\phi(x)]$.

Applications V.8. Lignes de niveaux :
- Point parabolique : si $Hf(0)$ est définie positive (resp. négative), alors f admet un minimum strict (resp. maximum strict) en 0, et les ligne de niveau sont difféomorphes à des cercles.
- Point hyperolique : si $Hf(0)$ est définie mais n'est ni positive, ni négative, alors le graphe de f traverse sont plan tangent.

• V.C Première et seconde forme fondamentale d'une surface

On considère U un ouvert de $\mathbb{R}^2$ et $\phi : U \to \mathbb{R}^3$ un plongement C^∞. On note $S = \phi(U)$ la surface définie par f.

Définition V.9. La *première forme fondamentale* au point $x \in U$, notéé$I(x)$, est la forme quadratique sur $\mathbb{R}^2$ définit par $I(x)[h] = \|D\phi(x)\|^2$.

Proposition V.10. L'application $I : U \to Q(E)$ est C^∞ et à valeur dans $Q^{++}(E)$.

L'application de Gauss est le champs de vecteurs normals sur S : $N(\phi(x)) = \frac{\partial_1\phi(x)\wedge\partial_2\phi(x)}{\|\partial_1\phi(x)\wedge\partial_2\phi(x)\|}$.

Définition V.11. La deuxième la *fonction de Weingarten* au point x est
$$\begin{array}{rccc} W(x): & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & x & \longmapsto & D\phi(x)^{-1}.DN(\phi(x)).D\phi(x).u \end{array}.$$

Proposition V.12. Pour $x \in U$, l'endomorphisme $W(x)$ est symétrique par rapport au produit scalaire $I(x)$.

Définition V.13. La *deuxième forme fondamentale* au point x est la forme quadratique
$$\begin{array}{rccc} II(x): & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & u & \longmapsto & -{}^t u.I(x).W(x).u \end{array}.$$

Définition V.14. La courbure de Gauss au point $x \in U$ est $K(x) = \det_{I(x)} II(x) = \det_{I(x)} W(x)$ et la courbure moyenne est $H(x) = Tr_{I(x)}(II(x)) = Tr(W(x))$.

Proposition V.15. Si $K(x) > 0$, alors S est localement ne traverse pas son plan tangent, le traverse si $K(x)$.

VI Développements

- Lemme de Morse.
- Théorème de John.
- Théorème de stabilité de Liapounov.
- Sous-groupe compact de $GL_n(\mathbb{R})$.
- $PLS_2(\mathbb{R}) \simeq O_0(2,1)$.
- Quadriques dans $M_2(\mathbb{R})$.
- Théorème de Pascal.
- Théorème d'Hermite.

149 - Groupes finis de petit cardinal.

Références [...]

I Dévissage des groupes finis

• I.A Sous-groupes distingués

Définition I.1. Soit G un groupe. Un sous-groupe H est *distingué* s'il est stable par conjugaison.

Définition I.2. Simplicité.

[A completer]

• I.B Produit semi-direct

Définition I.3. Produit semi directe de sous-groupes et de groupes abstraits ...

Proposition I.4. Caractérisation ...

II Liste des groupes d'ordre ≤ 15

Théorème II.1. Soit p un nombre premier.
- Tout groupe d'ordre p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
- Tout groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ ou $\mathbb{Z}/p^2\mathbb{Z}$.

Théorème II.2. Soient $p < q$ deux nombres premiers et G un groupe d'ordre pq
- Si $p \nmid q-1$, alors $G = \mathbb{Z}/pq\mathbb{Z}$.
- Si $P|q-1$, alors $G\mathbb{Z}/pq\mathbb{Z}$ ou $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

Théorème II.3. Développement Soit G un groupe d'ordre 12. Alors G est isomorphe à l'un des 5 groupes suivants
- Groupes abéliens : $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
- Groupes non-abéliens : $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \rtimes D_4 \simeq D_{12}$, $D_4 \rtimes \mathbb{Z}/3\mathbb{Z} \simeq \mathfrak{A}_4$.

III Étude de $\mathfrak{S}_n$

Proposition III.1.
- $\mathfrak{S}_n = \mathfrak{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$.
- Pour $n \neq 4$, $\mathfrak{A}_n$ est simple.
- $\mathfrak{A}_5 = D_4 \rtimes \mathbb{Z}/3\mathbb{Z}$.

Théorème III.2. Développement $\mathfrak{A}_5$ est les seul groupe simple d'ordre 60.

Théorème III.3. Pour $n \neq 6$, les automorphismes de $\mathfrak{S}_n$ sont intérieurs..

IV Groupes des polyèdres

Théorème IV.1. Développement Groupe des isométries des polyèdres ...

Théorème IV.2. Sous-groupes finis de $SO_3(\mathbb{R})$.

V Développements

- Groupe d'ordre 12.
- Groupe du dodécadèdre.
- Groupe d'ordre 60.

Références

[AB] JM Arnaudiès and J. Bertin. Groupes, Algebres et Geometrie.

[Aud06] M. Audin. *Geometrie*. EDP Sciences Editions, 2006.

[Ave92] A. Avez. *La lecon de géométrie à l'oral de l'agrégation*. Masson Editions, 1992.

[Ber77] M. Berger. *Geometrie*. Cedic, 1977.

[Cal06] J. Calais. *Eléments de théorie des anneaux : anneaux commutatifs*. Ellipses, 2006.

[Com98] F. Combes. *Algèbre et géométrie*. Bréal, 1998.

[Dem97] M. Demazure. *Cours d'algèbre : primalité, divisibilité, codes*. Cassini, 1997.

[Gob95] R. Goblot. *Algebre linéaire*. Masson, 1995.

[Gob96] R. Goblot. *Algèbre commutative*. Masson, 1996.

[Gou94] X. Gourdon. *Les maths en tête : algebre*. Ellipse, 1994.

[Lan02] S. Lang. Algebra, volume 211 of Graduate Texts in Mathematics, 2002.

[MT86] R. Mneimné and F. Testard. *Introduction à la théorie des groupes de Lie classiques*. Hermann, 1986.

[Per96] D. Perrin. *Cours d'algébre*. Ellipse, 1996.

[Tau] P. Tauvel. cours d'algèbre, dunod, 1999, 512.1 TAU.

[Tau97] P. Tauvel. Géométrie pour l'agrégation interne, 1997.