Université Paris-Sud
Mathématiques générales (algèbre).
D4M4U9, 2008/2009

Plan du cours.

1. Théorie des corps

1.1. Définitions, premières propriétés

Par définition, un corps est un anneau *commutatif* non nul dans lequel tout élément non nul est inversible. Exemples : $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Q}$, $\mathbf{Z}/p\mathbf{Z}$ avec p premier. Sous-corps, morphismes de corps (un tel morphisme est toujours injectif). Corps des fractions d'un anneau intègre.

1.2. Caractéristique d'un corps

Par définition, la caractéristique d'un corps K est l'entier $n \geq 0$ tel que le noyau du morphisme $\mathbf{Z} \to K$, $m \mapsto m.1_K$ soit $n\mathbf{Z}$. C'est 0 ou un nombre premier p. Notion de sous-corps premier de K (il est isomorphe à $\mathbf{Q}$ en caractéristique zéro, à $\mathbf{Z}/p\mathbf{Z}$ en caractéristique $p > 0$). Exemples (noter en particulier $\mathbf{Z}/p\mathbf{Z}(T)$, qui est infini mais de caractéristique $p > 0$). Notion de corps parfait.

1.3. Corps et espaces vectoriels

Notion d'extension de corps, d'extension finie. Degré d'une extension finie. Théorème de la "base télescopique", avec le corollaire : multiplicativité des degrés. Notations $K[\alpha]$ et $K(\alpha)$ quand L est une extension d'un corps K et $\alpha \in L$. Notion d'élément *algébrique* et *transcendant* sur un corps K, exemples (on remarquera que l'ensemble $\overline{\mathbf{Q}}$ des nombres complexes algébriques sur $\mathbf{Q}$ est dénombrable).

Polynôme minimal d'un élément algébrique (il est irréductible). Révision de la notion d'idéal d'un anneau commutatif et d'anneau quotient. En particulier, si P est irréductible sur un corps K, l'anneau $K[X]/(P)$ est un corps. Isomorphisme de K-algèbres $K[X]/(\pi_\alpha) \to K[\alpha]$ quand α est un élément algébrique sur K de polynôme minimal π_α.

Équivalence entre α algébrique sur K, $K[\alpha] = K(\alpha)$, et $K[\alpha]$ de dimension finie sur K. L'ensemble des éléments de L algébriques sur K est un corps

F, appelé *fermeture algébrique* de K dans L. Quand L est algébriquement clos, F l'est aussi et c'est la *clôture algébrique* de K. Par exemple $\overline{\mathbf{Q}}$ est un corps algébriquement clos dénombrable.

1.4. Corps de rupture, corps de décomposition

Notion de corps de rupture d'un polynôme *irréductible* $P \in K[X]$: c'est un corps $L = K[\alpha]$ avec α racine de P. Le corps de rupture existe et est unique à K-isomorphisme près (on peut prendre $K[X]/(P)$), mais l'isomorphisme n'est pas "canonique" (par exemple $\mathbf{Q}(\sqrt[3]{2})$, $\mathbf{Q}(j\sqrt[3]{2})$, $\mathbf{Q}(j^2\sqrt[3]{2})$ sont trois corps de rupture sur $\mathbf{Q}$ de $X^3 - 2$ et ils ne sont pas égaux en tant que sous-corps de $\mathbf{C}$). Le degré $[L : K]$ d'un corps de rupture L de P est $\deg P$.

Corps de décomposition d'un polynôme P de $K[X]$: c'est le "plus petit" corps sur lequel P est scindé. Il existe et est unique à isomorphisme près. En général il n'est pas isomorphe au corps de rupture (par exemple le corps de décomposition de $X^3 - 2$ sur $\mathbf{Q}$ est de degré 6 sur $\mathbf{Q}$).

1.5. Corps finis

Tout corps fini est de caractéristique $p > 0$, et son cardinal est p^n, où n est son degré sur son sous-corps premier. Réciproquement il existe un corps fini de cardinal p^n (unique à isomorphisme près) : c'est le corps de décomposition sur $\mathbf{Z}/p\mathbf{Z}$ du polynôme $X^{p^n} - X$. Il est noté $\mathbf{F}_{p^n}$. Bien noter que $\mathbf{F}_{p^n}$ n'est pas isomorphe comme anneau à $(\mathbf{Z}/p\mathbf{Z})^n$, ni à $\mathbf{Z}/p^n\mathbf{Z}$ (ils ne sont même pas intègres !).

Si P est un polynôme irréductible de degré n dans $\mathbf{Z}/p\mathbf{Z}[X]$, alors $\mathbf{F}_{p^n}$ est isomorphe au corps de rupture $\mathbf{Z}/p\mathbf{Z}[X]/(P)$ de P. Le corps $\mathbf{F}_{p^n}$ est une extension du corps $\mathbf{F}_{p^m}$ si et seulement si m divise n (par exemple $\mathbf{F}_8$ n'est pas une extension de $\mathbf{F}_4$).

2. Réduction des endomorphismes

On désigne toujours par E un espace vectoriel de dimension finie $n > 0$ sur un corps K.

2.1. Notions de base

Vecteurs propres, valeurs propres, spectre d'un endomorphisme u de E. Les valeurs propres sont les racines du *polynôme caractéristique* χ_u de u, qui est

unitaire de degré n. u est trigonalisable ssi χ_u est scindé. La somme des sous-espaces propres est directe, et la dimension de chaque sous-espace propre est au plus égale à la multiplicité de la valeur propre correspondante comme racine de χ_u. Si u et v commutent, alors u laisse stable les sous-espaces propres de v.

2.2. Endomorphismes diagonalisables

On dit que u est *diagonalisable* ssi il admet une matrice diagonale dans une certaine base. C'est équivalent à dire que la somme des sous-espaces propres est E tout entier, ou encore que χ_u est scindé avec la multiplicité de chaque valeur propre égale à la dimension du sous-espace propre correspondant. C'est en particulier le cas si u admet n valeurs propres distinctes. Exemples en dimension 2 sur $\mathbf{R}$, sur $\mathbf{C}$.

2.3. Polynômes d'endomorphismes

Polynôme minimal Π_u d'un endomorphisme $u \in \mathcal{L}(E)$, sous-algèbre $K[u]$ de $\mathcal{L}(E)$. Cas d'une matrice diagonalisable. Théorème de Cayley-Hamilton (Π_u divise χ_u, ou encore $\chi_u(u) = 0$). En corollaire, les valeurs propres sont aussi les racines du polynôme minimal. Théorème de décomposition des noyaux, et son corollaire fondamental : u est diagonalisable ssi Π_u est scindé à racines simples. Exemple des sous-groupes finis de $\mathrm{GL}_n(\mathbf{C})$, des matrices nilpotentes. Théorème de co-diagonalisation pour une famille d'endomorphismes diagonalisables commutant deux à deux.

2.4. Cas où χ_u est scindé

Théorème de décomposition en sous-espaces caractéristiques pour un endomorphisme u tel que χ_u soit scindé. Réduction d'un tel endomorphisme sous forme d'un tableau diagonal de matrices de la forme $\lambda_i I + N_i$, où λ_i est une valeur propre de u et N_i est nilpotente. Application : écriture (unique) $M = D + N$ d'une matrice M telle que χ_M soit scindée (D diagonalisable, N nilpotente, $ND = DN$).

Réduction de Jordan d'un endomorphisme nilpotent (existence et unicité de la réduite de Jordan). Application : toute matrice complexe est semblable à sa transposée.

2.5. Cas général

Matrice compagnon $C(P)$ associée à un polynôme P unitaire. On a $\chi_{C(P)} =$

$\pi_{C(P)} = P$. Notion de *sous-espace cyclique* : c'est un sous espace du type $\mathrm{Vect}(x, u(x), ...)$, sa dimension est le degré du *polynôme minimal en x* (noté π_x, u étant sous-entendu) et la matrice de la restriction de u à un tel sous-espace est $C(\pi_x)$ dans une certaine base. Réciproquement, si $\chi_u = \pi_u$, alors u est cyclique (:=E est un sous-espace cyclique), via le "lemme du vecteur cyclique".

Théorème de décomposition en espaces cycliques : pour tout u on peut décomposer E en somme directe de sous-espaces cycliques F_i $(1 \leq i \leq r)$, tels que si P_i désigne le polynôme minimal (ou caractéristique) de $u_{|F_i}$, alors $P_r|P_{r-1}|...|P_1$. En particulier P_1 est le polynôme minimal de u et χ_u est le produit des P_i. De plus les P_i ne dépendent que de u, on les appelle les *invariants de similitude* de u. Matriciellement, cela signifie que toute matrice de $M_n(K)$ est semblable à une et une seule matrice du type $\mathrm{Diag}(C(P_1), ..., C(P_r))$ telle que les P_i satisfassent la condition de divisibilité ci-dessus.

Corollaires : une matrice est toujours semblable à sa transposée; deux matrices de $M_n(K)$ semblables dans $M_n(L)$ (où L est une extension de K) le sont dans $M_n(K)$; les facteurs irréductibles de χ_u et π_u sont les mêmes.

3. Le groupe linéaire

Ici E est toujours un espace vectoriel de dimension $n > 0$ sur un corps K.

3.1. Généralités

Définitions de GL(E), de SL(E) et de leurs analogues matriciels $\mathrm{GL}_n(K)$, $\mathrm{SL_n(K)}$. On a une suite exacte (scindée)

$$1 \to \mathrm{SL(E)} \to \mathrm{GL(E)} \to \mathrm{K}^* \to 1$$

et en particulier SL(E) est un sous-groupe distingué de GL(E).

3.2. Transvections, dilatations

Un élément $u \neq \mathrm{id}$ de GL(E) qui induit l'identité sur un hyperplan H de E est une dilatation ou une transvection (le premier cas correspond à $\det u \neq 1$, le second à $\det u = 1$). Caractérisations matricielles. Écriture explicite d'une transvection.

Les transvections engendrent SL(E). Les transvections et les dilatations engendrent GL(E).

3.3. Centres et sous-groupes dérivés

Si τ est une transvection de droite D et d'hyperplan H, alors $u\tau u^{-1}$ est une transvection de droite $u(D)$ et d'hyperplan $u(H)$. Le centre de GL(E) est le groupe des homothéties (de rapport non nul), celui de SL(E) est le groupe des homothéties de rapport λ avec $\lambda^n = 1$.

Notion de *sous-groupe dérivé* $D(G)$ d'un groupe G : c'est le sous-groupe engendré par les *commutateurs* $[x, y] := xyx^{-1}y^{-1}$. On a $D(G)$ distingué dans G, $G/D(G)$ abélien, et tout sous-groupe distingué H avec G/H abélien contient $D(G)$. Propriétés de conjugaison (notamment : deux transvections sont toujours conjuguées dans SL(E) en dimension au moins 3). Le sous-groupe dérivé de GL(E) est SL(E) sauf si $n = 2$ et K est de cardinal 2.; le sous-groupe dérivé de SL(E) est SL(E) sauf si $n = 2$ et K est de cardinal 2 ou 3.

3.4. Exemples

Définition de $\mathrm{PGL}_n(K)$ et $\mathrm{PSL_n(K)}$. Ce dernier groupe est simple sauf si $n = 2$ et K est de cardinal 2 ou 3 (preuve dans le cas $n \geq 3$ en DM). Calcul du cardinal de $\mathrm{GL}_n(K)$ pour K fini.

4. Espaces euclidiens et hermitiens

4.1. Généralités sur les espaces euclidiens

Notion de produit scalaire sur un $\mathbf{R}$-ev E : c'est par définition une forme bilinéaire symétrique définie positive. Exemple du produit scalaire canonique de $\mathbf{R}^n$. Inégalité de Cauchy-Schwarz, norme euclidienne. Un *espace euclidien* est un $\mathbf{R}$-ev de dimension finie $n > 0$, muni d'un produit scalaire $\langle , \rangle$.

4.2. Orthogonalité

Orthogonal $A^\perp$ d'une partie A d'un espace euclidien E. Isomorphisme de E sur E^* donné par $x \mapsto (y \mapsto \langle x, y\rangle)$. Si F est un sev de E, alors $E = F \oplus F^\perp$. Procédé de Gram-Schmidt pour passer d'une base quelconque à une base orthonormée, avec une matrice de passage triangulaire supérieure. Notion d'*isométrie* de E. En particulier les isométries sont les endomorphismes dont la matrice O, dans une base **orthonormée** de E, est *orthogonale*, i.e. vérifie ${}^tOO = I$. Groupes $O_n(\mathbf{R})$ des matrices orthogonales et $SO_n(\mathbf{R})$ des matrices orthogonales de déterminant 1.

4.3. Endomorphismes et matrices symétriques

Adjoint u^* d'un endomorphisme u : il est caractérisé par la propriété que pour tous x, y de E, on a $\langle u(x), y\rangle) = \langle x, u^*(y)\rangle)$. Dans une base **orthonormée**, la matrice de u^* est la transposée de celle de u.

Un endomorphisme est dit *symétrique* si $u = u^*$. Théorème spectral : un tel endomorphisme est diagonalisable dans une base orthonormée. Traduction matricielle : toute matrice **réelle** symétrique S s'écrit $S = ODO^{-1}$ avec O orthogonale et D diagonale. Une matrice réelle symétrique S est *positive* (resp. *définie positive*) si toutes ses valeurs propres sont ≥ 0 (resp. > 0). Traduction en termes d'endomorphismes.

4.4. Structure des isométries d'un espace euclidien

Description des isométries en dimension 2 (les isométries positives sont les rotations, les négatives sont les réflexions). Théorème de réduction en dimension n. Engendrement de $O(E)$ par les réflexions si $n \geq 2$, et de $SO(E)$ par les renversements si $n \geq 3$.

4.5. Espaces hermitiens

Notion de forme semi-linéaire et de *forme sesquilinéaire* sur un $\mathbf{C}$-ev. Produit scalaire hermitien, espace hermitien (=$\mathbf{C}$-ev de dimension finie $n > 0$, muni d'un produit scalaire hermitien). Exemple de $\mathbf{C}^n$, muni de $\langle x, y\rangle = \sum_{i=1}^{n} \bar{x}_i y_j$. Notion d'orthogonal d'une partie, procédé de Gram-Schmidt (les propriétés sont exactement les mêmes que dans le cas euclidien).

Groupe unitaire $U(E)$ d'un espace hermitien E : il s'agit du groupe des isométries de E, isomorphe au groupe $U_n(\mathbf{C})$ des *matrices unitaires* M, i.e. celles qui vérifient $M^*M = I$, où M^* est la *matrice adjointe* de M (=la transposé-conjuguée).

Adjoint u^* d'un endomorphisme u d'un espace hermitien E. Sa matrice dans une b.o.n. est la matrice adjointe de celle de u, et il est caractérisé par $\langle u(x), y\rangle = \langle x, u(y)\rangle$ pour tous vecteurs x, y de E. Théorème fondamental : tout endomorphisme *normal* u (i.e. tel que $uu^* = u^*u$) est diagonalisable en b.o.n. Cas particulier des endomorphismes hermitiens ($u^* = u$, les valeurs propres sont réelles), antihermitiens ($u^* = -u$, les valeurs propres sont imaginaires pures) et unitaires ($u^* = u^{-1}$, les valeurs propres sont de module 1). Notion d'endomorphisme hermitien positif, défini positif (tout à fait analogue au cas des endomorphismes symétriques dans un espace euclidien).

4.6. Introduction aux formes quadratiques et hermitiennes

Notion de forme quadratique q sur un espace vectoriel E de dimension finie (sur $\mathbf{R}$, mais à part le théorème de Sylvester, tout est valable sur un corps quelconque de caractéristique $\neq 2$). La *forme polaire de* q est la forme bilinéaire symétrique φ telle que $q(x) = \varphi(x, x)$. Notion de cône, de noyau de q, forme non dégénérée. Un sous-espace F vérifie $= F \oplus F^{\perp}$ ssi la *restriction de* q à F est non dégénérée.

Matrice d'une forme quadratique dans une base. Formule de changement de base : $B =^t PAP$, où B est la matrice dans la base d'arrivée, A celle dans la base de départ, et P la matrice de passage. *Rang* de q (c'est le rang de A; en particulier A est inversible ssi q est non dégénérée). Notion de matrices symétriques *congruentes* (=elles représentent la même forme quadratique dans deux bases différentes).

Sur $\mathbf{R}$, théorème d'inertie de Sylvester : dans une certaine base, la matrice de q est de la forme $\mathrm{Diag}(a_i)$ avec a_i dans $\{0, 1, -1\}$, et le nombre de 0, de 1, et de -1 ne dépend que de q.

Notion de *forme hermitienne* sur un $\mathbf{C}$-ev E de dimension finie : c'est une application $h : E \to \mathbf{R}$ qui s'écrit $h(x) = \varphi(x, x)$, où φ est une forme sesquilinéaire à symétrie hermitienne. Les propriétés sont exactement les mêmes que celles des formes quadratiques réelles. Seule la formule de changement de base est légèrement différente, elle devient $B = P^*AP$.