III Leçon 151 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

Défense du Plan

La notion d'espace vectoriel est née conceptuellement avec la géométrie affine et l'invention de la notion de coordonées. C'est la généralisation de cette notion de coordonées qui nous offre ce domaine si vaste.
La présente leçon qui se limitera à une étude de la notion de rang et de dimension propose deux parties assez distinctes.
La première est théorique et se porte exclusivement sur la notion de dimension et de rang. Elle est là pour poser des bases saines sur le sujet. Le but premier est de montrer les notions et les objets essentiels utilisés en algèbre linéaire. Le second est de montrer les liens qui peuvent exister avec des domaines précédemment connus comme la résolution d'équations ou le lien avec les matrices.
Pour cela, on redéfinit la notion de famille génératice, famille libre, celle de base. Ensuite, on montre le lien entre la dimension et la somme d'espace vectoriel.
Enfin, dans la deuxième partie, on montre une première application utilisant ces notions avec l'échelonnement de matrice et le pivot de Gauss au travers de la résolution des équations.

La deuxième partie est là, comme son nom l'indique pour montrer deux applications de la notion de dimension dans d'autres branches des mathématiques. Ce seront donc nos deux développements.
J'ai choisi, premièrement, de proposer une présentation de l'algorithme découvert par Berlekamp au milieu des années 60. Il a proposé un algorithme pour écrire un polynôme sous forme de produit d'irréductible.
C'est donc une application qui trouve toute sa place dans l'algèbre linéaire et le calcul formel. Elle des intérêts bien évident en informatique pour la rapidité de calcul par exemple.
La deuxième quant à elle, se place dans la théorie des nombres. La démonstration du théorème d'Artin utilise des notions de théorie des corps, d'extension de corps et d'algèbre linéaire. La dimension ici permet de montrer le caractère fini et donc algébrique d'une extension et celle ci n'est d'ailleurs pas vraiment intuitive à mon gout. Ce théorème trouverait sa place dans un cours qui parlerait de la théorie de galois ou à la fin d'un cours qui introduirait la théorie des extension de corps.

a Plan

On suppose connues les notions d'espaces vectoriels(ev), de sous espace vectoriel(sev) et d'espace engendré par une famille de vecteurs.
Si ce n'est précisé, $\mathbb{K}$ est un corps, E et F deux $\mathbb{K}$-espace vectoriel($\mathbb{K} - ev$) de dimension finis, $x \in E$, I une partie de $\mathbb{N}$ et f un endomorphisme de E.

a.1 Théorie de la dimension

Famille génératrice, famille libre, bases

Définition 28. Une famille $(x_i)_{i\in I}$ est dite génératrice si Vect($(x_i)_{i\in I}$=E

Définition 29. Un espace vectoriel est dit de dimension fini s'il admet une famille génératrice finie sinon on parle d'espace vectoriel de dimension inifie.

Exemple 12.
- $\mathbb{R}^2$ est engendré par ((0,1) ;(1,0)).
- $(X^i)_{i\in\mathbb{N}}$ forme une famille génératrice de $\mathbb{K}[X]$

Définition 30. $(x_i)_{i\in I}$ est une famille libre si pour toute combinaison linéaire telle que $\sum_{k\in I} \lambda_k x_i = 0$ alors pour tout $k \in I$, $_k = 0$
Sinon c'est une famille liée.

Définition 31. Une famille libre et génératrice est une base de E.

Lemme 11. Soit **F** une famille libre de E et $x \in E$.
Alors $\mathbf{F}^{'} = \{\mathbf{F} \cup \{\mathbf{x}\}\}$ est libre si et seulement si $x \notin Vect(\mathbf{F})$

Lemme 12. Soit **F** une famille génératrice de E.
Alors **F** est liée si et seulement si il existe un vecteur $x \in \mathbf{F}$ tel que $\mathbf{F}\backslash\{x\}$ est encore génératrice.

Théorème 20. (Extraction de la base)
Soit **F** une famille génératrice de E. Alors on peut extraire de **F** une base de E.

Notions de dimension

Proposition 19. Soit A un $\mathbb{K}$-ev admettant une base de cardinal fini. Alors toutes les bases de A ont même cardinal et le cardinal commun est le cardinal de A.

Théorème 21. (Base incomplète)
Soit L une famille libre de E et G une famille génératrice de E. Il existe une base B tel que $L \subset B \subset G$.

Corollaire 6. Tout espace vectoriel de dimension finie admet une base

Application 4. En reprenant les notations introduite plus haut, il existe $P \in \mathbb{K}[X]$ tel que $P(f) = 0$.

Somme d'espace Vectoriel

Proposition 20. Soit F un sev de E. On a $dimF \leq dimE$. Il y a égalité si $F = E$

Application 5. Pour montrer l'égalité entre deux espaces vectoriels il faut et il suffit de montrer une inclusion et l'égalité entre les dimensions.

Définition 32. Soient F et G deux sev de E. On appelle somme de F et G le sous espace de E définie par $F+G$=$\{x \in E$ tel que $\exists y \in F$ et $z \in G, x = y+z\}$. La somme est dite directe si la décomposition est unique et elle est noté $F \oplus G$. On dit que G est le supplémentaire de F dans E lorsque que $E = F \oplus G$.

Proposition 21. (Formule de Grassmann) dim(F+G)=dim(F)+dim(G)-dim$(F \cap G)$.

Théorème 22. Tout sous espace vectoriel de E admet un supplémentaire.

Théorème 23. $E = F \oplus G \Leftrightarrow F \cap G = \{0\}$ et dim E = dim F+ dim G.

a.2 Théorie autour de la notion de rang

Définition 33. Le rang d'une famille de vecteurs est la dimension de l'espace vectoriel engendré par cette famille. i.e rg(f)=dim(Im(f))

Application linéaire

Définition 34. Le rang d'une application linéaire f est la dimension de son image.

Remarque 7. Si $(e_1, \ldots, e_n)$ base de E alors Im(f) est engendré par $(f(e_1), \ldots, f(e_n))$ et rg(f)=dim(Im(f)).

Théorème 24. (Théorème du rang)
Soit f une application linéaire de E dans F. Alors dim E = dim (Ker f)+rg(f)

Corollaire 7. Si de plus E et F ont même dimension alors :
f injective $\Leftrightarrow$ f surjective $\Leftrightarrow$ f bijective

Contre-Exemple 2. $l^0(\mathbb{N})$ est l'espace vectoriel des suites $\mathbb{N}$ dans $\mathbb{C}$.
Soit S l'application qui à $v = (v_n) \in l^0(\mathbb{N})$ associe u_0=0 et $u_n + 1$=v_n. S est surjective mais non injective car S$(1, \ldots,)$=S$(0, \ldots,)$.

Lien avec les matrices

Définition 35. Le rang d'une matrice de $\mathbf{M}_{m,n}(\mathbb{K})$

Proposition 22. $A \in \mathbf{M}_{m,n}$ matrice de $f \in \mathbf{L}(E,F)$ dans un couple de base quelconque.
Alors rg(A)=rg(f).

Corollaire 8. $A \in GL_n(\mathbb{K})$ si et seulement si rg(A)=n

Proposition 23. Pour $P \in GL_n(\mathbb{K})$, $A \in \mathbf{M}_{m,n}(\mathbb{K})$ et $Q \in GL_n(\mathbb{K})$, rg(PA)=rg(AQ)=rg(A).

Proposition 24. $A, B \in \mathbf{M}_{m,n}(\mathbb{K})$. A est équivalente à B si et seulement si rg(A)=rg(B).

Corollaire 9. Une matrice et sa transposée ont même rang.

Corollaire 10. Soit $A \in \mathbf{M}_{m,n}(\mathbb{K})$, $r = rg(A) \geq 1$.
A est équivalente à la matrice diagonale $J_r = diag(1, \ldots, 1, 0, \ldots, 0)$(r zéros, m-r zéros).

Pivot de Gauss

Définition 36. On appelle pivot d'une ligne non nulle le coefficient non nuls situés dans la colonne la plus à gauche.
Une matrice est dite échelonné en ligne lorsqu'elle satisfait les conditions suivantes :

- si une ligne est nulle toutes les suivantes sont nulles
- le pivot d'une ligne est strictement plus à droite que les pivots d'une ligne précédantes.

Une matrice échelonné est dite réduite si de plus tout les pivots sont égaux à 1 et les pivots sont les coefficients non nuls de leurs colonnes.

Exemple 13.

$$\begin{pmatrix} 1 & 5 & 0 & 1 \\ 0 & 2 & 7 & 9 \\ 0 & 0 & 5 & 8 \end{pmatrix}$$

est échelonné alors que

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 4 & 5 \\ 0 & 0 & 3 \end{pmatrix}$$

ne l'est pas.

Théorème 25. $Gl_m(\mathbb{K})$ agit à gauche sur $\mathbf{M}_{m,n}$.
De plus, deux matrice A et B sont dans la même orbite
si et seulement si elles ont même noyau
si et seulement si elles sont dans la même orbite d'une matrice échelonné en ligne réduite et cette matrice est unique.

Remarque 8. Avec l'action à droite A et B sont dans la même orbite si et seulement si elles ont même image.

Proposition 25. Soit (E) un sytème d'équation linéaire à n inconnues du type :

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n} &= b_1 \\ \cdots & \\ a_{n,1}x_1 + \cdots + a_{n,n} &= b_n \end{cases}$$

Alors résoudre E équivaut à résoudre AX=B avec X est la transposée de $(x_1, \ldots, x_n)$, B=

$$\begin{pmatrix} b_1 \\ \cdots \\ b_n \end{pmatrix}$$

et $A = (a_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}$.

Proposition 26. L'ensemble des solution d'un système linéaire est invariant par action à gauche des matrices de permutations, dilatation ou transvection.

Proposition 27. Pour résoudre un système, on peut échelonner la matrice associé au système. Deux cas se présentent alors :

- Il existe une ligne du type $0x_1 + \cdots + x_n = b \neq 0$ alors il n'y a pas de solutions.
- On obtient une matrice échelonné avec comme dernier pivot $a_{m,s}$ avec $s \leq n$.
  Si s=n, alors il y a unicité de la solution sinon on fixe des valeurs pour $(x_{s+1}, \ldots, x_n)$ et on se ramène au cas s=n.

L'ensemble des solutions est donc un espace affine de dimension s passant par une solution particulière.

a.3 Applications de la dimension finie

Quelques isomorphismes entre espaces

Proposition 28. Deux $\mathbb{K}$-ev sont isomorphes si et seulement s'ils ont même dimension.

Exemple 14. $\mathbb{C} \cong \mathbb{R}^2$ ou $\mathbb{K}_n[X] \cong \mathbb{K}^{n+1}$

Contre-Exemple 3. $dim_{\mathbb{C}}\mathbb{C} = 1$ et $dim_{\mathbb{R}}\mathbb{R} = 1$ mais $\mathbb{C} \ncong \mathbb{R}$

Extensions de corps

Définition 37. Si K et L sont deux corps et un f un morphisme de corps de K dans L. On appelle un tel morphisme une extension.

Proposition 29. Si L extension de corps de $\mathbb{K}$ alors L est un $\mathbb{K}$-ev.

Proposition 30. Si $dim_{\mathbb{K}} L \leq \infty$ on pose $[L : \mathbb{K}] = dim_{\mathbb{K}}\mathbb{L}(\in \mathbb{N})$ appellé degré de L sur $\mathbb{K}$.

Corps Fini

Proposition 31. Si $\mathbb{K}$ corps fini alors son cardinal vaut p^n où p est sa caractéristique et $n = dim_{\mathbb{Z}\backslash p\mathbb{Z}}\mathbb{K}$.

Lemme 13. Soit $q = p^n$ avec $n \in \mathbb{N}$. Alors :

- S : $\mathbb{F}_q[X] \longrightarrow \mathbb{F}_q[X]$, $S(Q) = Q^q$ est $\mathbb{F}_q$-linéaire
- Si L extension de $\mathbb{F}_q$ alors $\forall x \in L$, $x^q = x \Leftrightarrow x \in \mathbb{F}_q$

Théorème 26. (Développement 1) (Algorithme de Berlekamp)
Soient $q = p^n$ avec p premier et $n \in \mathbb{N}^*$ et $P \in \mathbb{F}_q[X]$ qui est sans facteur carré.
On pose $P = \prod_{i=1}^{r} P_i$, la décomoosition en produit d'irréductible sur $\mathbb{F}_q[X]$.
Si $r = 1$, alors P est irréductible sinon il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tel que $pgcd(P, V - \alpha)$ soit un facteur non trivial de P.

Théorème 27. Soient $K \subset L \subset M$ des corps, $(e_i)_{i\in I}$ une base de L sur K, $(f_j)_{j\in J}$ une base de M sur L.
Alors la famille $(e_i f_j)_{(i,j)\in I\circ J}$ est une base de M sur K.

Corollaire 11. Dans la situation du théorème si les dégrés sont finis on a $[M : K] = [M : L][L : K]$

Lemme 14. (Développement 2)(Lemme de Dedekind)
Soient $n \geq 1$, K et L deux corps et soit $\varphi_1, \ldots, \varphi_n : K \longrightarrow L$ n-homomorphisme de corps distincts.
Alors $(\varphi_1, \ldots, \varphi_n)$ est libre sur L.

Théorème 28. (Développement 2)(Théorème d'Artin)
Soit L un corps et soit H un sous groupe fini du groupe des automorphismes de L.
Si on note L^H=$\{x \in L$ tel que $\sigma(x) = x, \forall \sigma \in H\}$ alors $L\backslash L^H$ est une extension finie de degré $[L : L^H] = |H|$.

b Développements

b.1 Algorithme de Berlekamp

On rappelle le théorème des restes chinois qui nous sera utile dans la démonstration :

Théorème 29. Soient $P_1, \dots, P_r \in \mathbb{F}_q[X]$ polynômes premiers entre eux deux à deux. On pose $P = \prod_{i=1}^{r} P_i$. Alors
$\begin{array}{ccc} \mathbb{F}_q\backslash(P) & \longrightarrow & \mathbb{F}_q\backslash(P_1) \times \cdots \times \mathbb{F}_q\backslash(P_r) \\ x(modP) & \longmapsto & (x(modP_1), \dots, x(modP_r)) \end{array}$

On énonce l'algorithme de Berlekamp :

Théorème 30. Soient $q = p^n$ avec p premier et $n \in \mathbb{N}^*$ et $P \in \mathbb{F}_q[X]$ qui est sans facteur carré. On pose $P = \prod_{i=1}^{r} P_i$, la décomoosition en produit d'irréductible sur $\mathbb{F}_q[X]$.
Si $r = 1$, alors P est irréductible sinon il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tel que $pgcd(P, V - \alpha)$ soit un facteur non trivial de P.

Preuve. Considérons T : $\begin{array}{ccc} \mathbb{F}_q[X] & \longrightarrow & \mathbb{F}_q[X]\backslash(P) \\ Q & \longmapsto & Q^q(modP) \end{array}$ Comme $S : Q \longmapsto Q^q$ et la projection canonique sont deux applications $\mathbb{F}_q$-linéaires on peut conclure que T est $\mathbb{F}_q$-linéaire par composition.
$\forall Q \in \mathbb{F}_q[X]$, $T(QP) = (QP)^q[P] = 0$ donc $(P) \subset Ker(T)$.
On peut alors factoriser T pour obtenir un $\mathbb{F}_q$-endormorphisme φ de $\mathbb{F}_q[X]\backslash(P)$ défini par $\varphi([Q]) = [Q^q]$ en notant $[\mathrm{Q}]$ la classe d'équivalence de Q.
Les (P_i) sont premiers entre eux donc d'après le théorème des restes chinois, il existe $\Psi : \mathbb{F}_q\backslash(P) \longrightarrow \mathbb{F}_q\backslash(P_1) \times \cdots \times \mathbb{F}_q\backslash(P_r)$
Et pour tout $1 \leq i \leq r$, $F_q\backslash(P_i)$ est un corps car P_i est irréductible.
On pose $f = \Psi \circ \varphi \circ \Psi^{-1}$ application linéaire vérifiant $\forall Q = (Q_1, \dots, Q_r) \in \mathbb{F}_q\backslash(P_1) \times \cdots \times \mathbb{F}_q\backslash(P_r)$, $f(Q) = (Q_1^q, \dots, Q_r^q)$ car Ψ préserve la multiplication.
Donc on a pour $Q \in Ker(f - I_d) \Leftrightarrow Q_i^q = Q_i$ pour tout $1 \leq i \leq r$.
Or pour tout $1 \leq i \leq r$, $\mathbb{F}_q\backslash(P_i)$ est une extension de $\mathbb{F}_q$ donc on a $Q_i^q = Q_i$
$\Leftrightarrow Q_i \in \mathbb{F}_q$.
Donc card(Ker$(f - I_d)$=q^r donc
dim(Ker$(\varphi - I_d)$)=dim(Ker(f-I_d))=r.

Supposons maintenant que $r \geq 2$, les polynômes constants modulo P forment un sous espace vectoriel de $\mathbb{F}_q\backslash(P)$ de dimension 1 et il est engendré par 1.
De plus dim(Ker$(\varphi - I_d)$=$r \geq 2$, il $V \in *\mathbb{F}_q[X]$ non constant modulo P tel que $V^q = V$ (mod P).
En particulier, pour tout $1 \leq i \leq r$, on a V^q= V (mod P_i).
On pose $\alpha_i = V(modP_i) \in \mathbb{F}_q$.
Si pour tout $1 \leq i, j \leq r$, $\alpha_i = \alpha_j$ alors il existe $\alpha \in \mathbb{F}_q$ tel que $V = \alpha$ (mod P_i) pour tout $1 \leq i \leq r$.
grâce à l'injectivité de Ψ, $V = \alpha$ (mod P) est impossible car on a supposé n'est pas constant modulo P.

Donc il existe deux indices i et j tel que $\alpha_i \neq \alpha_j$.
On pose alors Q=pgcd(P,V-α_i). Mais P_i divise P et (V-α_i) donc il divise aussi Q.
De plus, P_j ne divise pas Q car il ne divise pas V-α_i puisque $\alpha_i \neq \alpha_j$.
Donc $Q \neq 1$, $Q \neq P$ et Q est un facteur non trivial de P.

Remarque 9.
- C'est une preuve constructive qui fournit un algorithme de calcul. Ici il suffit de calculer le noyau de l'application linéaire $\varphi - I_d$.
  Il est itératif, il faut recommencer avec $P\backslash(V - \alpha)$ et il s'arrête quand dim(Ker($\varphi - I_d$)=1. Ce qui équivaut à la situation où le polynôme est irréductible.

b.2 Théorème d'Artin

Lemme de Dedekind On démontre tout d'abord un lemme dont la paternité revient à Dedekind :

Lemme 15. Soient $n \geq 1$, K et L deux corps et soit $\varphi_1, \ldots, \varphi_n : K \longrightarrow L$ n-homomorphisme de corps distincts.
Alors $(\varphi_1, \ldots, \varphi_n)$ est libre sur L.

Preuve. Par l'absurde, supposons $(\varphi_1, \ldots, \varphi_n)$ non libre.
On se donne $(\lambda_1, \ldots, \lambda_n) \in L^n - \{0\}$, avec un nombre minimal r d'éléments non nuls tel que $\sum_{i=1}^{n} \lambda_i \varphi_i = 0$.
On a nécessairement $r \geq 2$ et qui à renuméroter, on peut supposer $\lambda_1, \ldots, \lambda_r \neq 0$ et $\sum_{i=1}^{r} \lambda_i \varphi_i = 0$.
Soit $y \in K$ tel que $\varphi_1(y) \neq \varphi_2(y)$. On a une première égalité :
$\forall x \in K$, $\sum_{i=1}^{r} \lambda_i \varphi_i(x) = 0$.
Et une deuxième : $\sum_{i=1}^{r} \lambda_i \varphi_i(xy) = \sum_{i=1}^{r} \lambda_i \varphi_i(x)\varphi_i(y) = 0$.
On réalise la différence entre la 2e et $\varphi_1(y)$ fois la première :
$\sum_{i=2}^{r} \lambda_2(\varphi_1(y) - \varphi_2(y))\varphi_i = 0$.
On obtient une contradiction par minimalité car $\lambda_2(\varphi_1(y) - \varphi_2(y)) \neq 0$.
Donc $(\varphi_1, \ldots, \varphi_n)$ est libre sur L.

Théorème d'Artin

Théorème 31. Soit L un corps et soit H un sous groupe fini du groupe des automorphismes de L.
Si on note L^H=$\{x \in L$ tel que $\sigma(x) = x, \forall \sigma \in H\}$ alors $L \backslash L^H$ est une extension finie de degré $[L : L^H] = |H|$.

Preuve. Si on pose $m = [L : L^H]$, m est éventuellement infi et $n = |H|$.
But : Montrer que m=n.
Premièrement, par l'absurde, supposons $m < n$. On se donne $(x_1, \ldots, x_m)$ une L^H-base de L et on note $\sigma_1, \ldots, \sigma_n$ éléments de H.
On considère le système d'équations :
$\sum_{i=1}^{n} \sigma_i(x_j) y_i = 0, \forall j \in \{1, \ldots, m\}$.
Puisque le nombre d'équation est strictement inférieur au nombre d'inconnues, il existe une solution non nulle $(y_1, \ldots, y_n)$ au sytème.
Alors, pour tout $x = \sum_{j=1}^{m} \lambda_j x_j \in L$ avec $\lambda_j \in L^H$, pour tout $j \in \{1, \ldots, m\}$,
$\sum_{i=1}^{n} y_i \sigma_i(x) = \sum_{i=1}^{n} \sum_{j=1}^{m} y_i \sigma_i(x_j) \lambda_j = \sum_{j=1}^{m} \lambda_j (\sum_{i=1}^{n} y_i \sigma_i(x_j)) = 0$.
Or ceci est absurde d'après le lemme de Dedekind donc $m \leq n$.

Deuxièmement, supposons que m>n.
Il existe donc une famille $(x_1, \ldots, x_{n+1})$, de L sur L^H. Par le même raisonnement que précédemment, il existe une famille non nulle $(y_1, \ldots, y_{n+1})$ de L telle que :
$\forall i \in \{1, \ldots, n\}, \sum_{j=1}^{n+1} \sigma_i(x_j) y_j = 0$.
On choisit $(y_1, \ldots, y_{n+1})$ tel que le nombre r de ses composantes non nulles soit minimal et quitte à renuméroter, on suppose que $y_1, \ldots, y_r \neq 0$ et $y_{r+1}, \ldots, y_{n+1} =$

0.
On suppose que $y_1 = 1$. On a $\forall i \in \{1, \ldots, n\}, \sigma_i(x_1) + \sum_{k=2}^{r} \sigma_i(x_k) = 0(3)$. On fait agir $\sigma \in H$ sur le système pour obtenir :
$\forall i \in \{1, \ldots, n\}, \sum_{k=1}^{r} \sigma(\sigma_i(x_k)\sigma(y_k) = 0$ et comme $\forall f \in H, f \longmapsto \sigma \circ f$ réalise une permutation des éléments de H.
Donc le dernier système est équivalent à : $\forall i \in \{1, \ldots, n\}, \sigma_i + \sum_{k=2}^{r} \sigma_i(x_k)\sigma(y_k) = 0(4)$.
On réalise (3)-(4) : $\sigma_i(x_2)(y_2 - \sigma(y_2) + \cdots + \sigma_i(x_r)(y_r - \sigma(y_r)) = 0, \forall i \in \{1, \ldots, n\}$.
Donc par minimalité de r, $y_j - \sigma(y_j = 0, \forall j \in \{2, \ldots, r\}$ donc $\forall j \in \{2, \ldots, r\}, y_j \in L^H$.
Ainsi (3) devient $\forall i \in \{1, \ldots, n\}$ tel que $\sigma_i = id_L$, on a $x_1 + \sum_{k=2}^{r} x_k y_k = 0$.
Ce qui est absurde par hypothèèse sur $(x_1, \ldots, x_{n+1})$ car $y_j \in L^H$. Donc $m \leq n$.

On peut donc conclure que m=n et que $L \backslash L^H$ est une extension finie de degré $[L : L^H] = |H|$.

c Références

- X. GOURDON Algèbre 2^e édition.
- X. GOURDON Les maths en tête. Algèbre.
- D. PERRIN Cours d'algèbre.
- J. GRIFONE Algèbre linéaire 5^e édition.
- P. SAMUEL Théorie Algébrique des Nombres
- A. BOSTAN Algorithme efficace en calcul formel
- V. BECK Objectif Agreg