1.2 Théorème de Cayley-Hamilton et lemme de Nakayama

Soit A un anneau commutatif.

Thm 1 (Cayley-Hamilton*, 1858 resp. 1853) : Soient M un A-module de type fini et $u : M \to M$ un endomorphisme. Alors il existe un polynôme unitaire qui annule u, i.e. on a

$$u^n + a_1 u^{n-1} + \dots + a_n \mathrm{Id}_M = 0$$

pour des $a_i \in A$. De plus, si l'on a $u(M) \subseteq JM$ pour un idéal J de A, on peut trouver $a_i \in J^i$.

Dém. : Supposons que M est engendré par $m_1, \dots, m_n$ et que $u(M) \subseteq JM$ (p.ex. $J = A$). Nous avons

$$u(m_i) = \sum_{j=1}^{n} a_{ij} m_j \tag{1}$$

pour des $a_{ij} \in J$. Considérons M comme un module sur $A[X]$, où X agit par u. Écrivons

$$m = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix} \in M^n, \quad I_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \in M_n(A).$$

Alors (1) nous donne

$$(X \cdot I_n - A) \cdot m = 0 \tag{2}$$

dans M^n considéré comme $A[X]$-module. Soit $B \in M_n(A[X])$ la transposée de la comatrice de $X I_n - A$. Si on multiplie (2) à gauche par B, on obtient

---

*Arthur Cayley, 1821 (Richmond) – 1895 (Cambridge)
Sir William Rowan Hamilton, 1805 (Dublin) – 1865 (Dublin)

$$\det(X\cdot I_n - A)\cdot I_n \cdot m = 0.$$

Mais alors on a

$$\det(X\cdot I_n - A)\, m_i = 0, \quad 1 \le i \le n,$$

et $P(X) = \det(X\cdot I_n - A)$ annule M considéré comme $A[X]$-module.

Donc $P(u)$ est nul en tant qu'endomorphisme de M. ∎

Cor. 2 : Soit M un A-module de type fini.

a) Tout endomorphisme surjectif de M est bijectif.

b) Si M est libre de rang fini n, toute famille génératrice formée de n éléments est une base.

Remarque : Par b), on a : $A^n \cong A^m \Longrightarrow n = m$.

Ceci n'est pas vrai en général pour les anneaux non-commutatifs. Par exemple, si $\Lambda = \mathrm{End}_A(A^{(\mathbb{N})})$, on a un isom. de Λ-modules (à droite)

$$\Lambda \xrightarrow{\sim} \Lambda \oplus \Lambda$$

induit par tout isomorphisme de A-modules $A^{(\mathbb{N})} \xrightarrow{\sim} A^{(\mathbb{N})} \oplus A^{(\mathbb{N})}$.

Dém. du cor. : a) Soit $f : M \to M$ un endom. surjectif. On considère M comme un $A[X]$-module, où X agit par f. Pour $J = (X)$, on a $JM = M$ car f est surjectif. On applique le théorème de Cayley-Hamilton à $u = \mathrm{Id}_M$. On a

$$u^n + a_1 u^{n-1} + \dots + a_n = 0$$

pour des $a_i \in (X)$. Cela se récrit

$$\mathrm{Id}_M - f\cdot Q(f) = 0$$

pour un $Q \in A[X]$. Alors $Q(f)$ est inverse de f.

b) Résulte de a) : Si M est libre de base $e_1, \dots, e_n$ et $m_1, \dots, m_n$ est génératrice, alors l'endomorphisme

$$M \longrightarrow M,\ e_i \longmapsto m_i$$

est surjectif, donc bijectif; donc $m_1, \dots, m_n$ est une base. ✓

Cor. 3 : Si M est de type fini et $I \subseteq A$ un idéal t.q. $IM = M$, alors il existe $x \in I$ t.q. $(1-x)M = 0$.

Dém. : On applique le thm de Cayley-Hamilton à $u = \mathrm{id}_M$. On obtient

$$\mathrm{id}_M + a_1 \mathrm{id}_M + \dots + a_n \mathrm{id}_M = 0$$

et on pose $x = -a_1 - \dots - a_n$. ✓

Cor. 4 ("Lemme de Nakayama*", 1951) Soient I un idéal contenu dans $\mathrm{Rad}A$ et M un A-module de type fini.

a) Si $IM = M$, alors $M = 0$.

b) Si les images de $m_1, \dots, m_n \in M$ engendrent M/IM, alors $m_1, \dots, m_n$ engendrent M.

⚠ En général, le fait que M/IM soit de type fini n'implique pas que M soit de type fini (p.ex. k corps, $A = k[[X]]$, $I = (X)$, $M = \mathrm{Frac}A$)

Dém. du cor. : a) Par le corollaire précédent, il existe $x \in \mathrm{Rad}A$ t.q. $(1-x)M = 0$. Or l'élément $1-x$ est inversible. Donc $M = 0$.

b) Soit $N = M/Am_1 + \dots + Am_n$. Alors

$$N/IN = M/(IM + Am_1 + \dots + Am_n) = 0.$$

Donc $N = IN$ et $N = 0$ par a). Cela donne $M = Am_1 + \dots + Am_n$. ✓

---

* Nakayama, Tadashi (中山正), 1912 (Tokyo) – 1964 (Nagoya)

1.3 Extensions finies et entières

Soient A un anneau et B une A-algèbre.

Déf : B est une *A-algèbre de type fini* si, *en tant que A-algèbre*, elle est engendrée par un nombre fini d'éléments.
B est une *A-algèbre finie* si, *en tant que A-module*, elle est engendrée par un nombre fini d'éléments.
Un élément $x \in B$ est *entier sur A* s'il est annulé par un polynôme *unitaire* à coefficients dans A.
B est *entier sur A* si tout élément de B est entier sur A.
B est une *extension entière* de A si de plus l'appl. can. $A \longrightarrow B$ est injective.

Rque : B est une A-alg. de type fini ssi elle est quotient d'une algèbre de polynômes $A[X_1, \dots, X_n]$. Elle est finie ssi en tant que A-module, elle est quotient d'un module libre de type fini A^n.

Prop. 1 : Soit $A \hookrightarrow B$ une extension d'anneaux et $x \in B$.

$\Leftrightarrow$
i) x est entier sur A.
ii) $A[x]$ est une A-algèbre finie, libre comme A-module.
iii) Il existe une A-algèbre finie A' t.q. $A \subseteq A[x] \subseteq A' \subseteq B$.

Dém : i) $\Rightarrow$ ii) Si x est annulé par un polynôme unitaire P à coeff. dans A et de degré n, alors le A-module $A[x]$ est engendré librement par $1, x, \dots, x^{n-1}$ (division euclidienne par P!).
ii) $\Rightarrow$ iii) On prend $A' = A[x]$.
iii) $\Rightarrow$ i) On considère la multiplication par x :

$$u : A' \longrightarrow A', \quad a' \longmapsto xa'.$$

Comme A' est un A-module de type fini, d'après le thm de Cayley-Hamilton, il existe un polynôme unitaire $P \in A[X]$ t.q. $P(u) = 0$. Mais alors $P(x) = P(u).1$ s'annule. ✓

Cor. 2 : Toute extension finie $A \hookrightarrow B$ est entière.

Prop. 3 : Soient $A \hookrightarrow B \hookrightarrow C$ des homomorphismes d'anneaux injectifs.

a) $A \hookrightarrow B$ finie et $B \hookrightarrow C$ finie $\Rightarrow$ $A \hookrightarrow C$ finie

b) $y_1, \dots, y_n \in B$ entiers sur $A \Rightarrow A[y_1, \dots, y_n]$ finie sur A.

c) $A \hookrightarrow B$ entier et $B \hookrightarrow C$ entier $\Rightarrow$ $A \hookrightarrow C$ entier.

Dém. : a) Si B est engendré par $x_1, \dots, x_p$ comme A-module et C engendré par $y_1, \dots, y_q$ comme B-module, alors C est engendré par $x_i y_j$, $1 \le i \le p$, $1 \le j \le q$, comme A-module.

b) résulte de a) par récurrence sur n.

c) Soit $c \in C$. Comme c est entier sur B, on a

$$c^n + b_1 c^{n-1} + \dots + b_n = 0$$

pour des $b_i \in B$. Donc $A[c]$ est fini sur $A[b_1, \dots, b_n]$, qui est fini sur A, par b). Donc $A[c]$ est fini sur A, par a), et c entier sur A. ✓

Déf : Soit $A \hookrightarrow B$ une extension d'anneaux. La clôture entière de A dans B est l'ensemble $\tilde{A}$ des éléments de B entiers sur A.

A est intégralement clos dans B si $\tilde{A} = B$.

Si A est intègre, A est intégralement clos si A est intégralement clos dans son corps de fractions.

Lemme 4 : a) $\tilde{A}$ est une ss-algèbre de B.

b) $A \subseteq \tilde{A}$ est une extension entière.

c) On a $\tilde{\tilde{A}} = \tilde{A}$.

Dém. : a) Clairement, on a $A \subseteq \tilde{A}$. Pour $b_1, b_2 \in \tilde{A}$, on sait que $A[b_1, b_2]$ est fini sur A. Donc $1_A, b_1+b_2, -b_1, b_1 b_2$ sont dans $\tilde{A}$.

b) Par définition des extensions entières.

c) On a $\tilde{A} \subseteq \tilde{\tilde{A}}$. Comme les extensions $A \subseteq \tilde{A}$ et $\tilde{A} \subseteq \tilde{\tilde{A}}$ sont entières, $\tilde{\tilde{A}}$ est entier sur A. Donc $\tilde{\tilde{A}} \subseteq \tilde{A}$. ✓

Lemme 5 : Tout anneau factoriel est intégralement clos.

Dém. : Soient C un anneau factoriel et $r/s \in \mathrm{Frac}(C)$, où r et s sont premiers entre eux. Supposons que

$$(r/s)^n + c_1 (r/s)^{n-1} + \dots + c_n = 0$$

Alors on a

$$r^n + s \cdot (c_1 r^{n-1} + \dots + c_n s^{n-1}) = 0$$

Comme r et s sont premiers entre eux, s doit être inversible dans C. ✓

Prop. 6 : Soit $A \subseteq B$ une extension et P un polynôme unitaire à coefficients dans A. Si on a

$$P = Q \cdot R$$

pour des polynômes unitaires Q et R dans $B[X]$, alors les coefficients de Q et R sont entiers sur A.

Dém. : Soient $C_1 = B[T]/(Q)$ et $\alpha_1 \in C_1$ l'image de T. Alors $Q(\alpha_1) = 0$ et comme Q est unitaire, on a $Q = (X - \alpha_1) \cdot Q_1$ dans $C_1[X]$. Notons que C_1 est un B-module libre de base

$1, a_1, \dots, a_1^{(\deg Q)-1}$ puisque Q est unitaire (division euclidienne). En particulier, l'homomorphisme can. $B \to C$, est injectif. En itérant cette construction on construit une extension d'anneaux $B \hookrightarrow C$ telle que

$$Q = \prod (X - \alpha_i), \quad R = \prod (X - \beta_j)$$

dans $C[X]$. Les α_i et β_j sont entiers sur A (car annulés par P). Donc les coeff. de Q et R sont entiers sur A. ✓

Cor. 7 ("Lemme de Gauss*"): Supposons A intégralement clos.
Si $P \in A[X]$ est unitaire et se factorise $P = QR$ pour des polynômes unitaires Q, R à coeff. dans $\mathrm{Frac}(A)$, alors Q et R sont à coeff. dans A.

Prop. 8: A intégralement clos $\Rightarrow$ $A[X]$ intégralement clos.

Rque: La réciproque est vraie aussi (!).

Dém.: Nous avons $\mathrm{Frac}(A[X]) \xleftarrow{\sim} K(X)$, où $K = \mathrm{Frac}(A)$. Soit $F \in K(X)$ entier sur $A[X]$. Alors F est en particulier entier sur $K[X]$. Comme $K[X]$ est factoriel, on a $F \in K[X]$. Supposons que

$$F^n + a_1 F^{n-1} + \dots + a_n = 0$$

pour des $a_i \in A[X]$. Alors

$$F \cdot (F^{n-1} + a_1 F^{n-2} + \dots + a_{n-1}) = -a_n$$

dans $A[X]$. Pour pouvoir appliquer le lemme de Gauss, on aimerait

---

* Johann Carl Friedrich Gauss, 1777 (Brunswick) – 1855 (Göttingen)

remplacer F et $(F^{n-1}+\dots+a_{n-1})$ par des polynômes unitaires. Ecrivons

$$F = X^r + G$$

où r est en entier $> \deg F$ et $> \deg a_i$ pour $1 \le i \le n$. Alors

$$(X^r+G)^n + a_1 (X^r+G)^{n-1} + \dots + a_n = 0$$

et donc

$$G^n + b_1 G^{n-1} + \dots + b_n = 0,$$

où $$-b_n = X^{rn} + a_1 X^{r(n-1)} + \dots + a_n.$$

On a $$-b_n = (-G)(-G^{n-1} - a_1 G^{n-2} - \dots - a_{n-1})$$

et c'est une factorisation en un produit de deux polynômes unitaires. Par le lemme de Gauss, on a $-G \in A[X]$. Donc $F \in A[X]$. ✓

1.4 Lemme de normalisation de Noether

Soit k un corps. Soit A une k-algèbre.

Déf. : Des éléments $a_1, \dots, a_n$ de A sont

- <u>algébriquement liés</u> s'il existe un polynôme $0 \neq P \in k[X_1, \dots, X_n]$ t.q. $P(a_1, \dots, a_n) = 0$;
- <u>algébriquement indépendants</u> s'ils ne sont pas alg. liés, i.e. $\forall P \in k[X_1, \dots, X_n]$: $P(a_1, \dots, a_n) = 0 \Rightarrow P = 0$.

A est une <u>extension algébrique pure</u> si $A = k[a_1, \dots, a_n]$ pour des éléments alg. indép. $a_1, \dots, a_n$ de A.