III. ANNEAUX NOETHÉRIENS, FACTORIELS, PRINCIPAUX

Séances des 17, 23 et 24 octobre

10. Modules et anneaux noethériens

10.1. Anneaux et modules noethériens. — Soient A un anneau et M un A-module.

Proposition 10.1. — *Les conditions suivantes sont équivalentes.*

1) *Tout sous-module de* M *est de type fini ;*

2) *Toute suite croissante de sous-modules de* M *est stationnaire, c.-à-d., pour toute suite croissante de sous-modules*

$$\mathrm{N}_0 \subseteq \mathrm{N}_1 \subseteq \mathrm{N}_2 \subseteq \cdots$$

il existe un entier k *tel que* $\mathrm{N}_i = \mathrm{N}_k$ *pour tout* $i \geqslant k$.

3) *Toute famille non-vide de sous-modules de* M *admet un élément maximal.*

Démonstration. — 1) $\Rightarrow$ 2) Supposons 1) vérifiée et soit

$$(*) \qquad \mathrm{N}_0 \subseteq \mathrm{N}_1 \subseteq \mathrm{N}_2 \subseteq \cdots$$

une suite croissante de sous-modules. Posons $\mathrm{N} = \bigcup_{i\geqslant 0} \mathrm{N}_i$; c'est un sous-module de M. Par hypothèse, il est engendré par un nombre fini d'éléments $x_1, \ldots, x_k$. Alors, il existe un entier r tel que $x_1, \ldots, x_k$ appartiennent tous à N_r. Donc $\mathrm{N} = \mathrm{N}_r$ et la suite $(*)$ est stationnaire à partir du cran r.

2) $\Rightarrow$ 3) Supposons qu'une famille non-vide $\mathscr{F}$ de sous-modules de M ne possède pas d'élément maximal. Soit N_0 un élément de $\mathscr{F}$. Comme il n'est pas maximal, il est contenu strictement dans un élément N_1 de $\mathscr{F}$. Ce dernier

(0) Version du 24/10/06

n'étant pas maximal, par hypothèse, il est contenu strictement dans un élément N_2 de $\mathscr{F}$. On construit ainsi une suite strictement croissante

$$N_0 \subset N_1 \subset N_2 \subset \cdots$$

de sous-modules de M, en contradiction avec l'hypothèse 2).

3) $\Rightarrow$ 1) Soit N un sous-module de M et soit $\mathscr{F}$ la famille des sous-modules de type fini de N. Elle est non-vide, car elle contient le sous-module (0). Donc, elle possède un élément maximal N'. Soit $n \in N$ arbitraire. Alors $N' + An$ est un sous-module de N de type fini (car il est engendré par n et un système de générateurs de N'). Par maximalité de N', on a $N' = N' + An$, d'où $n \in N'$. Ceci montre que $N' = N$, et donc N est de type fini. La proposition est démontrée. □

Définition 10.2. — On dit que M est un module **noethérien** s'il vérifie les conditions équivalentes de la proposition précédente. (Ceci entraîne, en particulier, que M soit de type fini).

Définition 10.3. — On dit que l'anneau A est **noethérien** s'il est noethérien comme A-module, c.-à-d., si tout idéal de A est de type fini.

Rappelons le résultat déjà vu suivant (séances 2-3 octobre, Proposition 5.6).

Proposition 10.4. — *Soient* M *un* A*-module et* N *un sous-module.*

1) *Si* M *est de type fini,* M/N *l'est aussi.*

2) *Si* N *et* M/N *sont de type fini, alors* M *l'est aussi.*

Proposition 10.5. — *Soient* M *un* A*-module,* N *un sous-module, et* $Q = M/N$ *le module quotient.*

1) *Si* M *est noethérien,* N *et* Q *le sont aussi.*

2) *Réciproquement, si* N *et* Q *sont noethériens,* M *l'est aussi.*

Démonstration. — 1) Supposons M noethérien et soit N', resp. Q', un sous-module de N, resp. Q. Comme N' est un sous-module de M, il est de type fini. D'autre part, on a $Q' = M'/N$, où $M' = \pi^{-1}(Q')$ est un sous-module de M. Par hypothèse, M' est de type fini, donc Q' l'est aussi, d'après la proposition précédente.

2) Supposons N et $Q = M/N$ noethériens et notons π la projection $M \to Q$. Soit M' un sous-module arbitraire de M. Alors $M' \cap N$ est un sous-module de N, donc est de type fini. D'autre part,

$$\frac{M'}{M' \cap N} \cong \pi(M')$$

est un sous-module de Q, donc est de type fini. Par conséquent, d'après la proposition précédente, M′ est de type fini. Ceci montre que M est noethérien. □

Corollaire 10.6. — *Soit* $\mathrm{M}_1, \cdots, \mathrm{M}_n$ *un nombre fini de modules noethériens. Alors* $\mathrm{M}_1 \oplus \cdots \oplus \mathrm{M}_n$ *est noethérien.*

Démonstration. — Supposons d'abord $n = 2$. Alors M_1 est un sous-module de $\mathrm{M}_1 \oplus \mathrm{M}_2$ et, d'après le 1er théorème d'isomorphisme (corollaire 2.18), le module quotient $(\mathrm{M}_1 \oplus \mathrm{M}_2)/\mathrm{M}_1$ est isomorphe à M_2. Donc, dans ce cas, le résultat découle du point 2) de la proposition précédente.

Enfin, le cas général s'en déduit par récurrence, puisque pour tout $n \geqslant 3$ l'on a

$$\mathrm{M}_1 \oplus \cdots \oplus \mathrm{M}_n \cong (\mathrm{M}_1 \oplus \cdots \oplus \mathrm{M}_{n-1}) \oplus \mathrm{M}_n.$$

Le corollaire est démontré. □

Corollaire 10.7. — *Soient* A *un anneau noethérien et* M *un* A*-module de type fini. Alors* M *est noethérien.*

Démonstration. — Par hypothèse, il existe $x_1, \ldots, x_n \in \mathrm{M}$ tels que

$$\mathrm{M} = \mathrm{A}x_1 + \cdots + \mathrm{A}x_n.$$

Alors, l'application $\phi : \mathrm{A}^n \to \mathrm{M}$ définie par

$$\phi(a_1, \ldots, a_n) = a_1x_1 + \cdots + a_nx_n$$

est un morphisme surjectif de A-modules. Donc, d'après le théorème 2.16, M s'identifie au module quotient $\mathrm{A}^n/\operatorname{Ker}(\phi)$.

Or, d'après le corollaire précédent, A^n est noethérien, et donc M l'est aussi, d'après le point 1) de la proposition 10.5. □

10.2. Anneaux de polynômes. — Soit A un anneau commutatif. De la même façon qu'on a défini $\mathbb{R}[\mathrm{X}]$, on peut définir l'anneau de polynômes $\mathrm{A}[\mathrm{X}]$.

Définition 10.8. — L'anneau $\mathrm{A}[\mathrm{X}]$ est le groupe abélien formé de toutes les sommes finies $\sum_{i=0}^{d} a_i\mathrm{X}^i$, où $d \in \mathbb{N}$ et $a_i \in \mathrm{A}$, muni de la multiplication définie par :

$$(*) \qquad \left(\sum_{i=0}^{d} a_i\mathrm{X}^i\right)\left(\sum_{j=0}^{f} b_j\mathrm{X}^j\right) = \sum_{\ell=0}^{d+f}\left(\sum_{\substack{i,j\geqslant 0\\ i+j=\ell}} a_ib_j\right)\mathrm{X}^\ell.$$

En particulier, $(a1)(b1) = (ab)1$ et donc A s'identifie à un sous-anneau de $\mathrm{A}[\mathrm{X}]$ et $\mathrm{A}[\mathrm{X}]$ est un A-module.

De plus, tout élément $P \neq 0$ dans $A[X]$ s'écrit de façon unique $P = a_n X^n + \cdots + a_0$, avec $a_n \neq 0$. On dit que n est le degré de P (noté $\deg P$), et que a_n est le coefficient dominant de P.

Proposition 10.9. — *Supposons* A *intègre. Alors, pour tout* $P, Q \in A[X] \setminus \{0\}$,

$$\deg(PQ) = \deg P + \deg Q.$$

En particulier, A[X] *est intègre et ses éléments inversibles sont les éléments inversibles de* A.

Démonstration. — Soient $P, Q \in A[X] \setminus \{0\}$, de termes dominants aX^d et bX^f, respectivement, où $d = \deg P$ et $f = \deg Q$. Comme A est intègre, $ab \neq 0$ et donc PQ est de degré $d + f$. En particulier, $PQ \neq 0$.

De plus, si P est inversible, d'inverse Q, l'égalité $PQ = 1$ entraîne $\deg P = \deg Q = 0$, et donc P et Q sont des éléments inversibles de A. La proposition est démontrée. □

Théorème 10.10 **(Division euclidienne par un polynôme unitaire)**

Soit $U \in A[X] \setminus \{0\}$ *un polynôme dont le coefficient dominant est* **inversible**. *Alors, on peut faire dans* A[X] *la division euclidienne par* U, *c.-à-d., pour tout* $P \in A[X]$, *il existe un unique couple* (Q, R) *d'éléments de* A[X] *tels que* $P = UQ + R$ *et* $\deg R < \deg U$.

On appelle Q *et* R *le quotient et le reste de la division euclidienne de* P *par* U.

Démonstration. — *Unicité.* Soient (Q, R) et (Q', R') deux couples vérifiant les propriétés ci-dessus. Alors, on a

$$(*) \qquad U(Q - Q') = R' - R.$$

Si $Q - Q'$ était non nul, disons de degré n, alors, puisque le coefficient dominant de U est inversible, $U(Q - Q')$ serait de degré $n + \deg U \geqslant \deg U$. Or, $R' - R$ est, par hypothèse, de degré $< \deg U$. Donc, nécessairement, $Q = Q'$ et $R = R'$. Ceci prouve l'unicité.

Existence. Écrivons $U = \alpha X^d + a_{d-1}X^{d-1} + \cdots + a_0$. Par hypothèse, le coefficient dominant α est inversible dans A. Montrons l'existence par récurrence sur $n = \deg P$.

Si $n < d$, on peut prendre $Q = 0$ et $R = P$. On peut donc supposer $n \geqslant d$ et l'existence démontrée pour tout polynôme de degré $< n$. Écrivons

$$P = b_n X^n + \cdots + b_0.$$

Alors, $P - b_n \alpha^{-1} U X^{n-d}$ est de degré $< n$. Donc, par hypothèse de récurrence, il existe $Q_0, R \in A[X]$, avec $\deg R < d$ tels que

$$P - b_n \alpha^{-1} U X^{n-d} = UQ_0 + R.$$

Alors, $\mathrm{P} = \mathrm{U}(\mathrm{Q}_0 + b_n\alpha^{-1}\mathrm{X}^{n-d}) + \mathrm{R}$. Ceci montre l'existence. Le théorème est démontré. □

On va généraliser la construction de l'anneau de polynômes A[X] au cas de n indéterminées $\mathrm{X}_1, \ldots, \mathrm{X}_n$. Commençons par le cas $n = 2$, c.-à-d., le cas de deux indéterminées X et Y.

Définition 10.11. — Soit A[X, Y] le A-module libre de base les monômes $\mathrm{X}^r\mathrm{Y}^s$, pour $(r, s) \in \mathbb{N}^2$. On définit le degré d'un tel monôme comme étant $r + s$.

Tout élément non nul $\mathrm{P} \in \mathrm{A}[\mathrm{X}, \mathrm{Y}]$ est une somme finie de termes $a_{r,s}\mathrm{X}^r\mathrm{Y}^s$, avec $a_{r,s} \in \mathrm{A}$, et le plus grand des degrés $r + s$ tel que $a_{r,s} \neq 0$ s'appelle le degré de P et se note $\deg \mathrm{P}$; ainsi P peut s'écrire comme somme finie

$$\mathrm{P} = \sum_{\substack{(r,s)\in\mathbb{N}^2 \\ r+s\leqslant n}} a_{r,s}\mathrm{X}^r\mathrm{Y}^s,$$

où $n = \deg \mathrm{P}$. On munit A[X, Y] de la multiplication définie par

$$\left(\sum_{\substack{(r,s)\in\mathbb{N}^2 \\ r+s\leqslant m}} a_{r,s}\mathrm{X}^r\mathrm{Y}^s\right)\left(\sum_{\substack{(t,u)\in\mathbb{N}^2 \\ t+u\leqslant n}} b_{t,u}\mathrm{X}^t\mathrm{Y}^u\right)$$

$$= \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^2 \\ \alpha+\beta\leqslant m+n}} \left(\sum_{\substack{(r,s),(t,u)\in\mathbb{N}^2 \\ r+t=\alpha,\, s+u=\beta}} a_{r,s}b_{t,u}\right)\mathrm{X}^\alpha\mathrm{Y}^\beta.$$

Ceci se généralise de façon évidente au cas de n variables. Toutefois, pour alléger l'écriture, il est utile d'observer que $\mathbb{N}^n$ est muni de l'addition définie composante par composante par :

$$(\nu_1, \ldots, \nu_n) + (\eta_1, \ldots, \eta_n) = (\nu_1 + \eta_1, \ldots, \nu_n + \eta_n).$$

De plus, pour tout $\nu = (\nu_1, \ldots, \nu_n)$ dans $\mathbb{N}^n$, on pose $|\nu| = \nu_1 + \cdots + \nu_n$ et l'on note X^ν le monôme

$$\mathrm{X}_1^{\nu_1} \cdots \mathrm{X}_n^{\nu_n};$$

il est de degré $|\nu|$. On peut alors définir l'anneau de polynômes $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ comme suit.

Proposition 10.12. — *Soit* $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *le* A*-module libre de base les monômes*

$$\mathrm{X}^\nu := \mathrm{X}_1^{\nu_1} \cdots \mathrm{X}_n^{\nu_n},$$

pour $\nu \in \mathbb{N}^n$*, un tel monôme étant de degré* $|\nu|$.

Tout élément $\mathrm{P} \in \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *est une somme finie de termes* $a_\nu \mathrm{X}^\nu$*, avec* $a_\nu \in \mathrm{A}$*, et le plus grand des degrés* $|\nu|$ *tels que* $a_\nu \neq 0$ *s'appelle le degré de* P *et se note* $\deg \mathrm{P}$ *; ainsi* P *peut s'écrire comme somme finie*

$$\mathrm{P} = \sum_{\substack{\nu \in \mathbb{N}^r \\ |\nu| \leqslant n}} a_\nu \mathrm{X}^\nu,$$

où $n = \deg \mathrm{P}$*. On munit* $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *de la multiplication définie par*

$$\left(\sum_{\substack{\nu \in \mathbb{N}^r \\ |\nu| \leqslant m}} a_\nu \mathrm{X}^\nu \right) \left(\sum_{\substack{\eta \in \mathbb{N}^r \\ |\eta| \leqslant n}} b_\eta \mathrm{X}^\eta \right) = \sum_{\substack{\mu \in \mathbb{N}^r \\ |\mu| \leqslant m+n}} \left(\sum_{\substack{\nu, \eta \in \mathbb{N}^r \\ \nu + \eta = \mu}} a_\nu b_\eta \right) \mathrm{X}^\mu.$$

Rappelons la définition déjà vue suivante (Chap. II, 7.2).

Définition 10.13. — Soient A, B deux **anneaux commutatifs**. On dit que B est une **A-algèbre** si l'on s'est donné un morphisme d'anneaux $\phi : \mathrm{A} \to \mathrm{B}$. Dans ce cas, B est aussi un A-module, via

$$a \cdot b = \phi(a) b, \qquad \forall\, a \in \mathrm{A}, b \in \mathrm{B}.$$

Définition 10.14. — Soient $\phi : \mathrm{A} \to \mathrm{B}$ et $\psi : \mathrm{A} \to \mathrm{C}$ deux A-algèbres. Un **morphisme de A-algèbres** $f : \mathrm{B} \to \mathrm{C}$ est un morphisme d'anneaux tel que $f \circ \phi = \psi$.

Se rappelant que ϕ (resp. ψ) fait de B (resp. C) un A-module via $a \cdot b = \phi(a) b$ (resp. $a \cdot c = \psi(a) c$), la seconde condition équivaut à dire que f est A-linéaire, c.-à-d., vérifie $f(a \cdot b) = a \cdot f(b)$, pour tout $a \in \mathrm{A}$, $b \in \mathrm{B}$.

Remarque 10.15. — Si A est un sous-anneau de B et de C, un morphisme de A-algèbres $f : \mathrm{B} \to \mathrm{C}$ est simplement un morphisme d'anneaux $f : \mathrm{B} \to \mathrm{C}$ tel que $f(a) = a$, pour tout $a \in \mathrm{A}$.

Théorème 10.16 **(Propriété universelle de** $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$**)**
Soit $\rho : \mathrm{A} \to \mathrm{B}$ *une* A*-algèbre. Pour tout* n*-uplet* $(b_1, \ldots, b_n)$ *d'éléments de* B*, il existe un unique morphisme de* A*-algèbres*

$$\phi : \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \longrightarrow \mathrm{B}$$

prolongeant ρ *et tel que* $\phi(\mathrm{X}_i) = b_i$*, pour* $i = 1, \ldots, n$*.*

Démonstration. — Un tel morphisme, s'il existe, doit vérifier, pour tout $\mathrm{P} = \sum_{|\nu| \leqslant \deg \mathrm{P}} a_\nu \mathrm{X}^\nu$,

$$(*) \qquad \phi(\mathrm{P}) = \sum_{|\nu| \leqslant \deg \mathrm{P}} \rho(a_\nu) b_1^{\nu_1} \cdots b_n^{\nu_n}.$$

Réciproquement, l'application $\phi : \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \to \mathrm{B}$ définie par la formule $(*)$ est A-linéaire et vérifie $\phi(1) = 1$. Il reste à vérifier que $\phi(\mathrm{PQ}) = \phi(\mathrm{P})\phi(\mathrm{Q})$, pour tout $\mathrm{P}, \mathrm{Q} \in \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Par bilinéarité, il suffit de le vérifier lorsque $\mathrm{P} = \mathrm{X}^\nu$ et $\mathrm{Q} = \mathrm{X}^\eta$ sont des monômes. Mais alors c'est clair, car

$$\phi(\mathrm{X}^{\nu+\eta}) = b_1^{\nu_1+\eta_1} \cdots b_n^{\nu_n+\eta_n} = b_1^{\nu_1} \cdots b_n^{\nu_n} \cdot b_1^{\eta_1} \cdots b_n^{\eta_n}.$$

Ceci prouve le théorème. □

Corollaire 10.17. — *Pour tout $n \geqslant 1$, on a un isomorphisme de* A*-algèbres*

$$\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \cong (\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}])[\mathrm{X}_n].$$

Démonstration. — Posons $\mathscr{A} = \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ et $\mathscr{B} = \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}]$. D'après la propriété universelle de $\mathscr{A}$, il existe un (unique) morphisme de A-algèbres

$$\phi : \mathscr{A} \longrightarrow \mathscr{B}[\mathrm{X}_n] \quad \text{tel que} \quad \phi(\mathrm{X}_i) = \mathrm{X}_i, \qquad \forall\, i = 1, \ldots, n.$$

D'autre part, $\mathscr{B}$ est un sous-anneau de $\mathscr{A}$, donc $\mathscr{A}$ est une $\mathscr{B}$-algèbre et, d'après la propriété universelle de $\mathscr{B}[\mathrm{X}_n]$, il existe un unique morphisme de $\mathscr{B}$-algèbres

$$\psi : \mathscr{B}[\mathrm{X}_n] \longrightarrow \mathscr{A} \quad \text{tel que} \quad \phi(\mathrm{X}_i) = \mathrm{X}_i, \qquad \forall\, i = 1, \ldots, n.$$

Alors ϕ et ψ sont des isomorphismes réciproques. □

10.3. Le théorème de transfert de Hilbert. —

Théorème 10.18 **(Théorème de transfert de Hilbert)**. — *Si* A *est noethérien,* A[X] *l'est aussi.*

Démonstration. — Soit I un idéal non nul de A[X]. Soit D le sous-ensemble de A formé de 0 et des coefficients dominants des polynômes $\neq 0$ appartenant à I. On voit facilement que D est un idéal de A. Par hypothèse, il est engendré par des éléments $\alpha_1, \ldots, \alpha_r$.

Pour tout $i = 1, \ldots, r$, soit P_i un élément de I dont le coefficient dominant est α_i, et soit $d_i = \deg \mathrm{P}_i$. Soit d le plus grand des d_i, et soit M le sous-A-module de A[X] engendré par les monômes $1, \mathrm{X}, \ldots, \mathrm{X}^{d-1}$. Alors M est noethérien, d'après le corollaire 10.7.

Soit $\mathrm{N} = \mathrm{M} \cap \mathrm{I}$; c'est un sous-A-module de M. Alors N est de type fini, donc engendré comme A-module par des éléments $\mathrm{Q}_1, \ldots, \mathrm{Q}_s$. Alors, I est égal à l'idéal J engendré par

$$\mathrm{P}_1, \ldots, \mathrm{P}_r, \mathrm{Q}_1, \ldots, \mathrm{Q}_s.$$

En effet, montrons par récurrence sur n que tout élément $\mathrm{P} \neq 0$ de I, de degré n, appartient à J. C'est clair si $n < d$, car dans ce cas $\mathrm{P} \in \mathrm{N}$ donc est combinaison A-linéaire de $\mathrm{Q}_1, \ldots, \mathrm{Q}_s$. Soit donc $n \geqslant d$ et supposons l'assertion

établie pour tout $n' < n$. Soit $\mathrm{P} \in \mathrm{I} \setminus \{0\}$, de degré n, et soit α son coefficient dominant. Alors $\alpha \in \mathrm{D}$ donc il existe $a_1, \ldots, a_r \in \mathrm{A}$ tels que

$$\alpha = a_1\alpha_1 + \cdots + a_r\alpha_r.$$

Alors,

$$a_1\alpha_1\mathrm{X}^{n-d_1}\mathrm{P}_1 + \cdots + a_r\alpha_r\mathrm{X}^{n-d_r}\mathrm{P}_r$$

a pour terme dominant $\alpha\mathrm{X}^n$, et donc

$$\mathrm{P} - \sum_{i=1}^{r} a_i\alpha_i\mathrm{X}^{n-d_i}\mathrm{P}_i$$

est un élément de I de degré $< n$. Il appartient donc à J, par hypothèse de récurrence. Enfin, comme les P_i sont dans J, on a aussi $\mathrm{P} \in \mathrm{J}$. Ceci prouve le théorème. □

Remarque 10.19. — En anglais, le théorème précédent est appelé « Hilbert's Basis Theorem ».

Corollaire 10.20. — *Si* A *est noethérien, alors* $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *l'est aussi, pour tout* $n \in \mathbb{N}$.

Démonstration. — Ceci découle, par récurrence sur n, du théorème précédent et du corollaire 10.17. □

Soit $\rho : \mathrm{A} \to \mathrm{B}$ une A-algèbre commutative.

Définition et proposition 10.21. — *Soit* S *un sous-ensemble non vide de* B. *On note* A[S] *le sous-*A*-module de* B *engendré par tous les monômes*

$$(*) \qquad x_1^{\nu_1} \cdots x_n^{\nu_n}, \quad \textit{où} \quad n \in \mathbb{N}^*, x_i \in \mathrm{S}, \nu_i \in \mathbb{N}.$$

*C'est une sous-*A*-algèbre de* B*, et c'est la plus petite sous-*A*-algèbre contenant* S. *On l'appelle la* **sous-algèbre** *de* B **engendrée par** S.

Démonstration. — Comme le produit de deux monômes du type $(*)$ est encore un monôme de même type, on voit facilement que A[S] est une sous-algèbre contenant S. Réciproquement, soit C une sous-A-algèbre de B contenant S. Alors C contient tous les monômes de type $(*)$ et contient donc A[S]. Ceci démontre la proposition. □

Remarque 10.22. — Si S est un ensemble fini $\{x_1, \ldots, x_n\}$, ce qui sera le cas dans la pratique, alors A[S] est le sous-A-module de B engendré par les monômes

$$x^\nu := x_1^{\nu_1} \cdots x_n^{\nu_n}, \quad \text{où} \quad \nu \in \mathbb{N}^n.$$

Définition 10.23. — On dit que B est une **A-algèbre de type fini** si elle est engendrée comme A-algèbre par un nombre fini d'éléments $x_1, \ldots, x_n$. D'après ce qui précède, ceci signifie que tout élément de B peut s'écrire (de façon non unique en général) comme une combinaison A-linéaire finie de monômes $x_1^{\nu_1} \cdots x_n^{\nu_n}$.

Proposition 10.24. — B *est une* A*-algèbre de type fini* $\Leftrightarrow$ B *est isomorphe à un quotient d'une algèbre de polynômes* $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$.

Démonstration. — Supposons B engendrée comme A-algèbre par $x_1, \ldots, x_n$. D'après la propriété universelle de l'algèbre $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ (10.16), ρ se prolonge en un morphisme de A-algèbres $\phi : \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \to \mathrm{B}$ tel que $\phi(\mathrm{X}_i) = x_i$ pour $i = 1, \ldots, n$. Ce morphisme est surjectif (car les x_i engendrent B comme algèbre), donc induit un isomorphisme de A-algèbres

$$(*) \qquad \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathrm{I} \xrightarrow{\sim} \mathrm{B},$$

où $\mathrm{I} = \mathrm{Ker}(\phi)$. Réciproquement, si l'on a un isomorphisme $(*)$, notons x_i l'image dans B de X_i. Alors les x_i engendrent B comme A-algèbre. Ceci prouve la proposition. □

Théorème 10.25. — *Si* A *est noethérien, toute* A*-algèbre* B *de type fini est noethérienne.*

Démonstration. — Soit B une A-algèbre de type fini. D'après la proposition précédente, on a un isomorphisme

$$\mathrm{B} \cong \mathscr{A}/\mathrm{I}, \qquad \text{où } \mathscr{A} = \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n],$$

pour un certain $n \geqslant 1$, et où I est un idéal de $\mathscr{A}$.

D'après 10.20, $\mathscr{A}$ est noethérien et, d'après 10.5, B est noethérien comme $\mathscr{A}$-module, donc aussi comme B-module (puisque tout idéal de B est un sous-$\mathscr{A}$-module de B). Donc, B est un anneau noethérien. □

11. Anneaux factoriels, principaux, euclidiens

11.1. Divisibilité, éléments irréductibles. — Soit A un anneau commutatif **intègre**. Soit $\mathrm{A}^\times = \mathrm{A} \setminus \{0\}$ et soit

$$\mathbf{U} = \{u \in \mathrm{A}^\times \mid \exists\, v \in \mathrm{A}^\times \text{ tel que } uv = 1\},$$

le groupe des éléments inversibles de $\mathrm{A}^\times$.

Définition 11.1. — On dit que $a, a' \in \mathrm{A}$ sont **associés** s'il existe un élément inversible $u \in \mathbf{U}$ tel que $a' = ua$.

Lemme 11.2. — *Soient* $a, b \in \mathrm{A}$. *Les conditions suivantes sont équivalentes :*

1) *a divise b et b divise a ;*

2) *a et b engendrent le même idéal ;*

3) *a et b sont associés.*

Démonstration. — Il est clair que 3) $\Rightarrow$ 2) $\Leftrightarrow$ 1). Réciproquement, si $(a) = (b)$, il existe $\alpha, \beta \in \mathrm{A}$ tels que $b = \alpha a$ et $a = \beta b$. Alors, $b = \alpha\beta b$ et comme A est intègre il vient $\alpha\beta = 1$. Donc α et β sont inversibles. Ceci prouve le lemme. □

Définition 11.3. — Un élément $p \in \mathrm{A}^\times$ est dit **irréductible** s'il est non inversible, et vérifie la propriété suivante : si $p = ab$, avec $a, b \in \mathrm{A}$, alors a ou b est inversible.

Ceci équivaut à dire que $p \notin \mathbf{U}$ et que ses seuls diviseurs sont ses associés, et les inversibles.

Définition 11.4. — Un idéal I de A est **principal** s'il peut être engendré par un seul élément, c.-à-d., s'il existe $a \in \mathrm{A}$ tel que $\mathrm{I} = (a)$.

Un tel a s'appelle un générateur de I, et a est unique à un élément inversible près.

Proposition 11.5. — *Soit* I *un idéal principal non nul et distinct de* A. *Les conditions suivantes sont équivalentes :*

1) I *est engendré par un élément irréductible p ;*

2) I *est un élément maximal de l'ensemble des idéaux principaux* $\neq \mathrm{A}$ *;*

3) *tout générateur p de* I *est irréductible.*

Démonstration. — Supposons p irréductible et (p) contenu dans un idéal principal $(b) \neq \mathrm{A}$. Alors b n'est pas inversible, et il existe $a \in \mathrm{A}$ tel que $p = ab$. Comme p est irréductible, ceci entraîne que a est inversible, d'où $(b) = (p)$. Ceci prouve l'implication 1) $\Rightarrow$ 2).

Montrons que 2) $\Rightarrow$ 3). Supposons (p) maximal parmi les idéaux principaux $\neq \mathrm{A}$ et supposons $p = ab$. Alors $(p) \subseteq (a)$ et deux cas sont possibles.

Si $(a) = \mathrm{A}$, alors a est inversible et b associé à p. D'autre part, si $(a) = (p)$, alors $p = ua$, avec $u \in \mathrm{A}^\times$ (d'après le lemme), et donc $ab = p = ua$, d'où $b = u$ puisque A est intègre. Ceci montre que p est irréductible. L'implication 2) $\Rightarrow$ 3) est démontrée.

Enfin, 3) $\Rightarrow$ 1) est clair. La proposition est démontrée. □

Théorème 11.6 **(Existence d'une décomposition en facteurs irréductibles)**

Soit A *un anneau commutatif intègre* **noethérien**. *Alors, tout élément non nul et non inversible de* A *est un produit fini d'éléments irréductibles.*
(*En particulier, si* A *n'est pas un corps, il existe des éléments irréductibles.*)

Démonstration. — Si A est un corps, c.-à-d., si tout élément de $\mathrm{A} \setminus \{0\}$ est inversible, il n'y a rien à montrer. Sinon, considérons l'ensemble d'idéaux suivant :

$\mathscr{I} := \{(a) \mid a \in \mathrm{A}^\times$ est non inversible et n'est pas un produit fini d'éléments irréductibles$\}$

La proposition sera démontrée si on montre que cet ensemble $\mathscr{I}$ est vide.

Supposons $\mathscr{I}$ non vide. Il admet alors un élément maximal (a), où $a \in \mathrm{A}^\times$ n'est ni inversible ni un produit fini d'éléments irréductibles. En particulier, a n'est pas irréductible, donc il existe b, c dans A, tous deux non inversibles, tels que $a = bc$. Donc

$$(a) \subseteq (b), \qquad (a) \subseteq (c),$$

et chacune de ces inclusions est stricte. En effet, si on avait $(a) = (b)$, il existerait $d \in \mathrm{A}$ tel que $b = ad$, d'où $a = bc = adc$ et $1 = dc$ (car A est intègre), et c serait inversible, une contradiction. Donc l'inclusion $(a) \subset (b)$ est stricte, et il en est de même de $(a) \subset (c)$.

Donc, comme (a) est un élément maximal de $\mathscr{I}$, et comme b et c sont non inversibles, alors b et c sont chacun un produit fini d'éléments irréductibles, et il en est de même de leur produit $bc = a$! Ceci contredit l'hypothèse $(a) \in \mathscr{I}$, et cette contradiction montre que $\mathscr{I} = \varnothing$. Le théorème est démontré. □

Remarque 11.7. — 1) En général, on n'a pas unicité de la décomposition en facteurs irréductibles. Par exemple :

a) Dans $\mathbb{Z}[i\sqrt{5}] = \mathbb{Z}[\mathrm{X}]/(\mathrm{X}^2 + 5)$, on a

$$(2 + i\sqrt{5})(2 - i\sqrt{5}) = 9 = 3 \cdot 3,$$

et l'on peut montrer que $2 + i\sqrt{5}$, $2 - i\sqrt{5}$ et 3 sont irréductibles mais deux à deux non associés ; voir [**Pe1**, p.II.8] et 11.6 plus loin.

b) Dans $\mathrm{A} = \mathbb{C}[\mathrm{X}, \mathrm{Y}]/(\mathrm{X}^2 - \mathrm{Y}^3)$, notons x et y les images de X et Y. On a $x^2 = y^3$, et l'on peut montrer que x et y sont irréductibles et non associés.

2) Dans les deux cas précédents, il n'est pas si facile de montrer que les éléments en question sont irréductibles et non associés. Ceci peut se faire, par exemple, en considérant la norme associée à une extension quadratique, et en étudiant les factorisations possibles de la norme $\mathrm{N}(\alpha)$ d'un élément α. Voir [**Sa**, § II.5 & IV.5] et 11.6 plus loin.

3) Les anneaux intègres pour lesquels la décomposition en facteurs irréductibles existe et est unique (aux inversibles près), sont appelés anneaux **factoriels**. On les étudie dans le paragraphe suivant.

Définition 11.8. — Soient $a, b \in \mathrm{A}$. On dit que a et b sont **premiers entre eux** ou **sans facteur commun**, si tout diviseur commun à a et b est inversible. Ceci équivaut à dire que : A *est le seul idéal principal contenant* a *et* b.

Lemme 11.9. — *Soit* $p \in \mathrm{A}$ *irréductible et* $a \in \mathrm{A} \setminus \{0\}$. *Si* $a \notin (p)$ *alors* a *et* p *sont sans facteur commun.*

Démonstration. — Supposons que b soit non inversible et divise a et p. Alors, b est associé à p et il en résulte que p divise a, contradiction. Ceci prouve le lemme. □

Lemme 11.10. — *Soient* A *un anneau intègre et* p *un élément non nul de* A. *Si l'idéal* (p) *est premier, alors* p *est irréductible.*

Démonstration. — L'hypothèse que (p) soit un idéal premier, donc $\neq \mathrm{A}$, entraîne que p est non inversible.

Soient $a, b \in \mathrm{A}$ tels que $p = ab$. Comme (p) est premier, ceci entraîne, disons, que $a \in (p)$, d'où $a = p\alpha$, avec $\alpha \in \mathrm{A}$. Alors $p = p\alpha b$, et comme A est intègre il vient $\alpha b = 1$. Donc b est inversible. Ceci montre que p est irréductible. □

Notation 11.11. — On écrira $a \mid b$ (resp., $a \nmid b$) pour signifier que a divise (resp., ne divise pas) b.

11.2. Anneaux factoriels, lemmes d'Euclide et Gauss. —

Définition 11.12. — Soit A un anneau commutatif. On dit que A est **factoriel** s'il est **intègre** et vérifie les deux conditions suivantes : **existence** (E) et **unicité** (U) de la **décomposition en facteurs irréductibles**, c.-à-d.,

(E) Tout $a \in \mathrm{A} \setminus \{0\}$, non inversible, s'écrit

$$a = p_1 \cdots p_r,$$

où $r \geqslant 1$ et les p_i sont des éléments irréductibles de A ;

(U) La décomposition précédente est unique au sens suivant : si l'on a deux décompositions

$$a = p_1 \cdots p_r = q_1 \cdots q_s,$$

où les p_i et les q_j sont irréductibles, alors $s = r$ et il existe une permutation $\sigma \in \mathrm{S}_r$ telle que p_i et $q_{\sigma(i)}$ soient associés, pour tout $i = 1, \ldots, r$. C.-à-d., de façon plus concise, la décomposition est unique à l'ordre des termes et aux inversibles près.

On rappelle que (E) est satisfaite si A est noethérien (Proposition 11.6). Mais il y a aussi des exemples d'anneaux factoriels qui ne sont pas noethériens, c.-à-d., la décomposition en facteurs irréductibles peut exister sans que A soit nécessairement noethérien.

Proposition 11.13. — *Soit* A *un anneau commutatif intègre vérifiant* (E). *Les propriétés suivantes sont équivalentes.*

1) A *vérifie* (U).

2) *Pour tout élément irréductible* $p \in \mathrm{A}$, *l'idéal* (p) *est premier.*

3) A *vérifie le* **Lemme d'Euclide**, *c.-à-d., si* $p \in \mathrm{A}$ *est irréductible et divise un produit* $ab \neq 0$, *il divise* a *ou* b.

4) A *vérifie le* **Lemme de Gauss**, *c.-à-d., pour tout* $a, b, c \in \mathrm{A} \setminus \{0\}$, *si* a *divise* bc *et si* a, b *sont sans facteur commun, alors* a *divise* c.

Démonstration. — Il est clair que 2) et 3) sont équivalents. L'implication 4) $\Rightarrow$ 3) est facile. En effet, soit p irréductible divisant un produit $ab \neq 0$. Si $p \nmid a$ alors, d'après le lemme 11.9, a et p sont sans facteur commun, et l'hypothèse 4) donne alors que p divise b.

Montrons que 2) $\Rightarrow$ (U). Plus précisément, montrons que si l'on a une égalité

$$(*) \qquad p_1 \cdots p_m = u q_1 \cdots q_n,$$

où u est inversible et les p_i et q_j sont irréductibles, alors $m = n$ et il existe une permutation $\sigma \in \mathrm{S}_n$ telle que p_i et $q_{\sigma(i)}$ soient associés, pour $i = 1, \ldots, n$. On peut supposer $m \leqslant n$.

Si $m = 0$, le terme de gauche vaut 1 et ceci entraîne $n = 0$, car sinon q_1 serait inversible, ce qui n'est pas le cas pour un élément irréductible. Supposons $m > 0$ et le résultat établi pour $m - 1$.

Il résulte de $(*)$ que l'on a

$$\overline{q}_1 \cdots \overline{q}_n = 0$$

dans l'anneau $\mathrm{A}/(p_1)$; comme ce dernier est intègre, par hypothèse, on obtient que p_1 divise l'un des q_i, donc lui est associé (puisque q_i est irréductible). Donc, quitte à changer la numérotation des q_j, on peut supposer que $p_1 = v q_1$, avec v inversible. Alors, comme A est intègre, on déduit de $(*)$ l'égalité

$$p_2 \cdots p_m = uv q_2 \cdots q_n,$$

et le résultat cherché découle alors de l'hypothèse de récurrence. Ceci prouve que 2) $\Rightarrow$ (U).

Montrons maintenant que 1) $\Rightarrow$ 4). Supposons A factoriel et soient $a, b, c, d \in \mathrm{A} \setminus \{0\}$ tels que $ad = bc$, avec a et b sans facteur commun. Montrons que a divise c. On a des égalités

$$\begin{aligned} a &= \alpha p_1 \cdots p_n, & d &= \delta p'_1 \cdots p'_r, \\ b &= \beta q_1 \cdots q_s, & c &= \gamma q'_1 \cdots q'_t, \end{aligned}$$

avec $\alpha, \beta, \gamma, \delta$ inversibles, $n, r, s, t \geqslant 0$, et les p_i, p'_j, q_k et q'_ℓ irréductibles. On a donc une égalité

$$(**) \qquad u p_1 \cdots p_n \cdot p'_1 \cdots p'_r = q_1 \cdots q_s \cdot q'_1 \cdots q'_t,$$

avec u inversible. Montrons, par récurrence sur n, que ceci entraîne que $a \mid c$. Si $n = 0$, alors a est inversible et l'assertion est claire. Supposons $n \geqslant 1$ et le résultat établi pour $n - 1$.

Comme a et b sont sans facteur commun, p_1 ne peut être conjugué à l'un des q_j ; l'hypothèse (U) entraîne donc que p_1 est associé à un q'_k. Quitte à renuméroter les q'_k, on peut supposer que $p_1 = vq'_1$, avec v inversible. Alors, comme A est intègre, on déduit de $(**)$ l'égalité

$$uvp_2 \cdots p_n \cdot p'_1 \cdots p'_r = q_1 \cdots q_s \cdot q'_2 \cdots q'_t,$$

et le résultat cherché découle alors de l'hypothèse de récurrence. Ceci prouve que si A vérifie (E) et (U), il vérifie 4). Ceci achève la démonstration de la proposition. □

Remarque 11.14. — a) En procédant comme ci-dessus, on peut démontrer directement l'implication : A factoriel $\Rightarrow$ 3).

b) Ce qu'on appelle Lemme d'Euclide, resp. de Gauss, est l'assertion que si A est factoriel, il vérifie la condition 3), resp. 4). Pour mémoire, énonçons ci-dessous ces deux lemmes sous leur forme usuelle.

Proposition 11.15. — *Supposons* A *factoriel et soient* $a, b, c \in \mathrm{A} \setminus \{0\}$ *tels que* a *divise* bc.

(Lemme d'Euclide) *Si* a *est irréductible, il divise* b *ou* c.

(Lemme de Gauss) *Si* a *est sans facteur commun avec* b, *il divise* c.

Remarque 11.16. — Le Lemme de Gauss est **équivalent** à l'assertion $(*)$ ci-dessous :

$(*)$ Si a et b sont sans facteur commun et divisent x, alors ab divise x.

En effet, soient $a, b \in \mathrm{A}$ sans facteur commun. Supposons que A vérifie le Lemme de Gauss et que a, b divisent x. Alors x égale bc et est divisible par a. Comme a et b sont premiers entre eux, a divise c, donc $c = ad$ et $x = bad$ est divisible par ab.

Réciproquement, supposons $(*)$ vérifiée et $x = bc$ divisible par a. Alors x est divisible par ab, d'où $x = abd$, et comme A est intègre il vient $c = ad$, donc a divise c.

Corollaire 11.17 **(Lemme de Gauss)**. — *Soit* A *factoriel, soient* $a_1, \ldots, a_n \in \mathrm{A}$, *deux à deux sans facteur commun, et soit* b *un multiple commun aux* a_i. *Alors* b *est divisible par* $a_1 \cdots a_n$.

Démonstration. — On procède par récurrence sur n. Si $n = 2$, c'est la propriété $(*)$. Supposons $n \geqslant 3$ et le résultat établi pour $n - 1$. Par hypothèse de récurrence, il existe $c \in \mathrm{A}$ tel que

$$b = a_2 \cdots a_n c.$$

Alors, par application répétée du Lemme de Gauss, on obtient que a_1 divise c. Ceci prouve le corollaire. □

11.3. PPCM et PGCD dans un anneau factoriel. —

Remarque 11.18. — Soit A un anneau commutatif et soient $a_1, \dots, a_n \in \mathrm{A}$. L'ensemble des multiples communs aux a_i est égal à l'idéal

$$(a_1) \cap \cdots \cap (a_n).$$

D'autre part, un élément d de A divise tous les a_i si, et seulement si, (d) contient l'idéal $(a_1, \dots, a_n)$ engendré par les a_i.

Définition et proposition 11.19. — *Soit* A **factoriel** *et soient* $a_1, \dots, a_n \in \mathrm{A}^\times$.

1) *L'idéal* $\mathrm{I} := (a_1) \cap \cdots \cap (a_n)$ *est principal. Soit* M *un générateur de cet idéal* (M *est unique à multiplication par un inversible près, c.-à-d., tout autre générateur de* I *est associé à* M) *; alors* M *est un multiple commun aux* a_i*, qui divise tout multiple commun des* a_i*. On dit que* M *est un* **PPCM** *(plus petit commun multiple) des* a_i*. Par abus de notation, on écrira* $\mathrm{M} = \mathrm{ppcm}(a_1, \dots, a_n)$.

2) *L'ensemble des idéaux principaux contenant* $(a_1, \dots, a_n)$ *possède un unique élément minimal* J*. Tout générateur* d *de* J *est un diviseur commun aux* a_i*, et si* f *est un autre diviseur commun aux* a_i*, alors* (f) *contient* $\mathrm{J} = (d)$ *et donc* f *divise* d*. Donc,* d *est un diviseur commun aux* a_i*, qui est divisible par tout diviseur commun des* a_i*. Par conséquent, tout élément associé à* d *est un* **PGCD** *(plus grand commun diviseur) des* a_i*. Par abus de notation, on écrira* $d = \mathrm{pgcd}(a_1, \dots, a_n)$.

De façon plus concrète, en décomposant chaque a_i *en produits d'irréductibles, on peut écrire :*

$$(\dagger) \qquad \begin{cases} a_1 = u_1\, p_1^{c_{11}} \cdots p_r^{c_{1r}}, \\ \quad \vdots \qquad\qquad \vdots \\ a_n = u_n\, p_1^{c_{n1}} \cdots p_r^{c_{nr}}, \end{cases}$$

où $p_1, \dots, p_r \in \mathrm{A}$ *sont des éléments irréductibles deux à deux non associés,* $u_1, \dots, u_n \in \mathrm{A}$ *sont inversibles, et* $c_{ij} \in \mathbb{N}$*. Pour* $j = 1, \dots, r$*, posons*

$$\mathrm{M}_j = \max\{c_{1j}, \dots, c_{nj}\}, \quad m_j = \min\{c_{1j}, \dots, c_{nj}\},$$

et soient

$$\mathrm{M} = p_1^{\mathrm{M}_1} \cdots p_r^{\mathrm{M}_r}, \qquad d = p_1^{m_1} \cdots p_r^{m_r}.$$

Alors M *est un générateur de* I*, donc un PPCM des* a_i*. D'autre part, tout diviseur commun aux* a_i *divise* d*, et donc* d *est un PGCD des* a_i*.*

Démonstration. — Soit $b \in \mathrm{A}$ un multiple commun aux a_i. Dans la décomposition (†), fixons un indice $j \in \{1, \dots, r\}$. Alors, b est divisible par $p_j^{c_{ij}}$,

pour $i = 1, \dots, n$, donc aussi par M_j. Comme les $p_j^{\mathrm{M}_j}$ sont deux à deux sont diviseurs communs, il résulte du corollaire 11.17 que b est divisible par

$$\mathrm{M} := p_1^{\mathrm{M}_1} \cdots p_r^{\mathrm{M}_r}.$$

Ceci montre que M engendre l'idéal $(a_1) \cap \cdots \cap (a_n)$ et est donc un PPCM des a_i.

D'autre part, comme $a_i = u_i\, p_1^{c_{i1}} \cdots p_r^{c_{ir}}$, il résulte de l'unicité de la décomposition en facteurs irréductibles que tout diviseur de a_i est de la forme

$$a_i' = v_i\, p_1^{c'_{i1}} \cdots p_r^{c'_{ir}},$$

où v_i est inversible et $c'_{ij} \leqslant c_{ij}$ pour $j = 1, \dots, r$. Donc, si f est un diviseur commun aux a_i, alors

$$f = v\, p_1^{c'_1} \cdots p_r^{c'_r},$$

où v est inversible et où, pour chaque $j = 1, \dots, r$, c'_j est inférieur à c_{ij}, pour $i = 1, \dots, n$, donc à m_j. Par conséquent, f divise

$$d = p_1^{m_1} \cdots p_r^{m_r}.$$

Ceci montre que d est un PGCD des a_i. La proposition est démontrée. □

Définition 11.20. — On dit que $a_1, \dots, a_n \in \mathrm{A}$ sont **premiers entre eux** s'ils n'ont pas de diviseur commun non inversible. Ceci équivaut à dire que leur PGCD est 1.

Corollaire 11.21 **(Unicité de l'écriture des fractions)**. — *Soit* A *factoriel et soit* K *son corps des fractions.*

1) *Soient $x, y \in \mathrm{A} \setminus \{0\}$ et soit d un PGCD de x et y. Alors x/d et y/d sont sans facteur commun.*

2) *Tout élément $f \neq 0$ de* K *s'écrit de façon unique, aux inversibles près, $f = a/b$, avec $a, b \in \mathrm{A} \setminus \{0\}$ sans facteur commun.*

Démonstration. — 1) Écrivons $x = da$ et $y = db$. Si p était un élément non inversible divisant a et b, l'idéal (dp) contiendrait x et y et serait strictement contenu dans (d), contrairement à la définition de (d). Ceci prouve 1).

2) Soit $f \in \mathrm{K} \setminus \{0\}$. Par définition de K, il existe $x, y \in \mathrm{A} \setminus \{0\}$ tels que $f = x/y$. Soit d un pgcd de x et y ; posons $x = da$ et $y = db$. Alors a, b sont sans facteur commun, et $f = da/db = a/b$. Ceci prouve l'existence.

Montrons l'unicité, aux inversibles près. Supposons que $f = c/d$, avec c et d sans facteur commun. Alors, on a l'égalité

$$ad = bc.$$

Comme a, b (resp. c, d) sans sont facteur commun, il résulte du Lemme de Gauss que $a \mid c$ et $b \mid d$ (resp. $d \mid b$ et $c \mid a$). Par conséquent, a et c sont associés, de même que b et d. Ceci prouve le corollaire. □

11.4. Le théorème de transfert de Gauss. — Le but de cette section est de démontrer le théorème suivant.

***Théorème 11.22* (Théorème de transfert de Gauss).** —
Si A *est factoriel,* A[X] *l'est aussi.*

Corollaire 11.23. — *Si* A *est factoriel,* $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *l'est aussi.*

Démonstration. — Le corollaire découle du théorème par récurrence sur n, vu l'isomorphisme $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \cong (\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}])[\mathrm{X}_n]$. □

Pour la démonstration du théorème, on aura besoin de notions et résultats préliminaires. Démontrons d'abord la proposition suivante. Soit K le corps des fractions de A.

Proposition 11.24. — *Soit* A *intègre et soit* $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ *vérifiant l'une des deux conditions suivantes :*

i) P *est un élément irréductible de* A *;*

ii) $\deg \mathrm{P} \geqslant 1$*, les coefficients de* P *sont sans facteur commun, et* P *est irréductible en tant qu'élément de* K[X].

Alors P *est un élément irréductible de* A[X].

Démonstration. — Supposons $\mathrm{P} = \mathrm{QR}$, avec $\mathrm{QR} \in \mathrm{A}[\mathrm{X}]$.

1) Si P est un élément irréductible $p \in \mathrm{A}$, alors Q et R sont de degré 0, donc appartiennent à A, et l'irréductibilité de p entraîne que Q ou R est inversible. Ceci prouve que p est irréductible dans A[X].

2) Supposons ii) vérifiée. L'irréductibilité de P comme élément de K[X] entraîne, disons, que $\deg \mathrm{Q} = 0$. Donc Q appartient à A, et est un diviseur commun à tous les coefficients de P. Par conséquent, Q est inversible. Ceci prouve que P est un élément irréductible de A[X]. La proposition est démontrée. □

On aura besoin plus loin du lemme suivant. Soit I un idéal de A et notons IA[X] l'idéal de A[X] engendré par I. On observe que IA[X] est formé des polynômes dont tous les coefficients appartiennent à I.

Lemme 11.25. — *On a un isomorphisme de* A*-algèbres*

$$\mathrm{A}[\mathrm{X}]/\mathrm{IA}[\mathrm{X}] \xrightarrow{\sim} (\mathrm{A}/\mathrm{I})[\mathrm{X}].$$

Par conséquent, si I *est un idéal premier de* A*, alors* IA[X] *est un idéal premier de* A[X].

Démonstration. — Soit π la projection $\mathrm{A} \to \mathrm{A}/\mathrm{I}$; ceci fait de A/I une A-algèbre. D'après la propriété universelle de A[X], il existe un unique morphisme

de A-algèbres $\phi : \mathrm{A}[\mathrm{X}] \to (\mathrm{A}/\mathrm{I})[\mathrm{X}]$ tel que $\phi(\mathrm{X}) = \mathrm{X}$. Explicitement, pour tout $\mathrm{P} = a_0 + \cdots + a_d\mathrm{X}^d$, on a

$$\phi(\mathrm{P}) = \pi(a_0) + \cdots + \pi(a_d)\mathrm{X}^d.$$

Il est clair que ce morphisme est surjectif, et son noyau est l'idéal des polynômes dont tous les coefficients sont dans I, c.-à-d., $\mathrm{IA}[\mathrm{X}]$. Ceci prouve la première assertion. La deuxième en résulte, d'après la proposition 10.9. □

Désormais, on suppose que A est **factoriel**.

***Définition 11.26* (Contenu d'un polynôme)**. — Soit $\mathrm{P} \in \mathrm{A}[\mathrm{X}] \setminus \{0\}$. On note $c(\mathrm{P})$ et l'on appelle **contenu** de P un pgcd de ses coefficients. (Ainsi, le contenu est défini à un inversible près). On dit que P est **primitif** si $c(\mathrm{P})$ est inversible, c.-à-d., si les coefficients de P sont sans facteur commun.

Remarque 11.27. — Soit $a \in \mathrm{A} \setminus \{0\}$. On voit facilement que $c(a\mathrm{P}) = ac(\mathrm{P})$.

***Lemme 11.28* (Lemme des contenus de Gauss)**. — *On a* $c(\mathrm{PQ}) = c(\mathrm{P})c(\mathrm{Q})$, *pour tout* $\mathrm{P}, \mathrm{Q} \in \mathrm{A}[\mathrm{X}] \setminus \{0\}$.

Démonstration. — On peut écrire $\mathrm{P} = c(\mathrm{P})\widetilde{\mathrm{P}}$ et $\mathrm{Q} = c(\mathrm{Q})\widetilde{\mathrm{Q}}$, où $\widetilde{\mathrm{P}}$ et $\widetilde{\mathrm{Q}}$ sont primitifs. Alors

$$\mathrm{PQ} = c(\mathrm{P})c(\mathrm{Q})\widetilde{\mathrm{P}}\widetilde{\mathrm{Q}},$$

et donc $c(\mathrm{PQ}) = c(\mathrm{P})c(\mathrm{Q})c(\widetilde{\mathrm{P}}\widetilde{\mathrm{Q}})$, d'après la remarque précédente.

Par conséquent, on peut supposer P et Q primitifs, et il s'agit de montrer que PQ l'est aussi. Supposons que ce ne soit pas le cas, et soit p un élément irréductible divisant $c(\mathrm{PQ})$.

Alors, dans l'anneau $\mathrm{A}[\mathrm{X}]/p\mathrm{A}[\mathrm{X}]$, on a $\overline{\mathrm{PQ}} = 0$. Mais, d'après le lemme 11.25, l'on a

$$\mathrm{A}[\mathrm{X}]/p\mathrm{A}[\mathrm{X}] \cong (\mathrm{A}/p\mathrm{A})[\mathrm{X}],$$

et cet anneau est intègre, car $p\mathrm{A}$ est un idéal premier de A puisque A est factoriel. Par conséquent, on a $\overline{\mathrm{P}} = 0$ ou $\overline{\mathrm{Q}} = 0$, et donc p divise tous les coefficients de P ou de Q, ce qui contredit l'hypothèse que P et Q sont primitifs. Cette contradiction montre que PQ est primitif, et le lemme est démontré. □

Nous pouvons maintenant démontrer le théorème de transfert de Gauss. On suppose A factoriel.

Montrons que A[X] vérifie (E). Considérons d'abord un élément primitif $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$, de degré $\geqslant 1$. Vu comme élément de K[X], P s'écrit :

$$\mathrm{P} = \mathrm{P}_1^{n_1} \cdots \mathrm{P}_r^{n_r},$$

où les P_i sont des polynômes irréductibles de K[X] de degré $\geqslant 1$. Pour chaque i, on peut écrire $\mathrm{P}_i = (a_i/b_i)\widetilde{\mathrm{P}}_i$, avec $a_i, b_i \in \mathrm{A} \setminus \{0\}$ et $\widetilde{\mathrm{P}}_i \in \mathrm{A}[\mathrm{X}]$ primitif. De plus, chaque $\widetilde{\mathrm{P}}_i$ est, comme P_i, irréductible dans K[X]. Donc, d'après la

proposition 11.24, chaque $\widetilde{\mathrm{P}}_i$ est un élément irréductible de A[X]. De plus, on a l'égalité

$$(b_1^{n_1}\cdots b_r^{n_r})\,\mathrm{P} = (a_1^{n_1}\cdots a_r^{n_r})\,\widetilde{\mathrm{P}}_1^{n_1}\cdots\widetilde{\mathrm{P}}_r^{n_r}.$$

Prenant les contenus, on voit que $b_1^{n_1}\cdots b_r^{n_r}$ et $a_1^{n_1}\cdots a_r^{n_r}$ sont associés. Par conséquent,

$$\mathrm{P} = u\widetilde{\mathrm{P}}_1^{n_1}\cdots\widetilde{\mathrm{P}}_r^{n_r},$$

avec $u \in \mathrm{A}$ inversible, et ceci est une décomposition de P en facteurs irréductibles.

Enfin, soit $\mathrm{P} \in \mathrm{A}[\mathrm{X}] \setminus \{0\}$ arbitraire. On peut écrire $\mathrm{P} = c(\mathrm{P})\widetilde{\mathrm{P}}$, où $\widetilde{\mathrm{P}}$ est primitif. Alors $\widetilde{\mathrm{P}}$ admet une décomposition comme ci-dessus, et, d'autre part, $c(\mathrm{P}) \in \mathrm{A}$ se décompose en produit d'irréductibles. Ceci prouve que A[X] vérifie (E).

Conséquence. Le résultat de décomposition qu'on vient de démontrer implique le résultat suivant :

(†) Soit P un élément irréductible de A[X]. Alors ou bien : *i)* $\deg \mathrm{P} = 0$ et $\mathrm{P} = p$ est un élément irréductible de A, ou bien : *ii)* $\deg \mathrm{P} \geqslant 1$ et P est primitif et irréductible dans K[X].

En effet, soit $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ irréductible. D'après ce qui précède, P s'écrit comme un produits d'irréductibles

$$\mathrm{P} = a_1\cdots a_r\mathrm{P}_1\cdots\mathrm{P}_s$$

avec les a_i de type *i)* et les P_j de type *ii)*. Comme P est irréductible, on a $r + s = 1$ et donc $\mathrm{P} = a_1$ ou bien $\mathrm{P} = \mathrm{P}_1$.

Pour montrer que A[X] est factoriel, il reste à montrer, d'après la proposition 11.13, que tout élément irréductible engendre un idéal premier. Si p est un élément irréductible de A, ceci résulte du fait que

$$\mathrm{A}[\mathrm{X}]/p\mathrm{A}[\mathrm{X}] \cong (\mathrm{A}/p\mathrm{A})[\mathrm{X}]$$

est intègre. D'autre part, soit $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ un élément irréductible de degré $\geqslant 1$. Supposons que P divise un produit QR, où $\mathrm{Q}, \mathrm{R} \in \mathrm{A}[\mathrm{X}]$.

Comme P est irréductible dans K[X], qui est factoriel, on peut supposer que P divise Q dans K[X]. Il existe donc $a, b \in \mathrm{A} \setminus \{0\}$ et $\mathrm{S} \in \mathrm{A}[\mathrm{X}]$ primitif tels que

$$(*) \qquad \mathrm{Q} = \frac{a}{b}\,\mathrm{SP},$$

d'où $b\mathrm{Q} = a\mathrm{PS}$. D'après le lemme des contenus, on obtient que

$$b\,c(\mathrm{Q}) = ac(\mathrm{PS}) = a,$$

d'où $a/b \in \mathrm{A}$. Alors $(*)$ montre que P divise Q dans A[X]. Ceci prouve que l'idéal (P) de A[X] est premier. Ceci termine la preuve du théorème de transfert de Gauss.

11.5. Anneaux principaux et anneaux euclidiens. —

Définition 11.29. — Soit A un anneau commutatif. On dit qu'il est **principal** s'il est **intègre** et si tout idéal de A est engendré par un élément.

***Lemme 11.30* (Théorème de Bezout)**. — *Soit* A *un anneau principal et soient* $x, y \in \mathrm{A}$ *sans facteur commun. Il existe* $a, b \in \mathrm{A}$ *tels que*

$$(*) \qquad 1 = ax + by.$$

Démonstration. — Soit $\mathrm{I} = \mathrm{A}x + \mathrm{A}y$. Comme A est principal, I est engendré par un élément d, de la forme $d = ax + by$. D'autre part, comme (d) contient x et y, alors d est un diviseur commun à x et y. L'hypothèse entraîne que d est inversible, d'où $\mathrm{A}x + \mathrm{A}y = \mathrm{A}$. Le lemme en découle. □

Corollaire 11.31. — *Soit* A *principal et soit* $p \in \mathrm{A}$ *irréductible. Alors* (p) *est maximal, donc premier.*

Démonstration. — Soit $a \in \mathrm{A}$ non divisible par p. Alors p et a sont sans facteur commun donc, d'après le lemme (théorème) de Bezout, il existe $u, v \in \mathrm{A}$ tels que $up + vb = 1$. Donc $(p) + \mathrm{A}a = \mathrm{A}$, pour tout $a \notin (p)$. Ceci montre que (p) est maximal. □

Théorème 11.32. — *Soit* A *un anneau principal. Alors :*

1) A *est noethérien et factoriel.*

2) *Tout idéal premier non nul de* A *est engendré par un élément irréductible, et est un idéal maximal.*

Démonstration. — Par hypothèse, A est intègre. Comme tout idéal de A est engendré par un élément, A est noethérien. En particulier, il vérifie la condition (E), d'après la proposition 11.6.

Soit p un élément irréductible de A. D'après le corollaire précédent, l'idéal (p) est maximal, donc a fortiori premier. D'après la proposition 11.13, ceci montre que A est factoriel.

Enfin, soit (a) un idéal premier non nul de A. D'après le lemme 11.10, a est irréductible, et l'on vient de voir que dans ce cas (a) est un idéal maximal. Le théorème est démontré. □

Des exemples importants d'anneaux principaux sont fournis par les anneaux euclidiens, introduits ci-dessous.

Définition 11.33. — Soit A un anneau commutatif. On dit que A est **euclidien** s'il est **intègre** et s'il existe une application $\rho : \mathrm{A}^\times \to \mathbb{N}$ vérifiant la propriété suivante : pour tout $a, b \in \mathrm{A} \setminus \{0\}$, il existe $q, r \in \mathrm{A}$ tels que

$$a = bq + r, \quad \text{et } r = 0 \text{ ou bien } \rho(r) < \rho(b).$$

Proposition 11.34. — *Tout anneau euclidien* A *est principal. Plus précisément, soit* I *un idéal non nul de* A *et soit* $a \in \mathrm{I}$ *tel que* $\rho(a)$ *soit minimal. Alors* $\mathrm{I} = (a)$.

Démonstration. — Soit I un idéal non nul de A. Alors l'ensemble des $\rho(\mathrm{P})$, pour $\mathrm{P} \in \mathrm{I} \setminus \{0\}$ est un sous-ensemble non vide de $\mathbb{N}$ donc admet un plus petit élément d. Soit $\mathrm{P}_0 \in \mathrm{I}$ tel que $\rho(\mathrm{P}_0) = d$ et soit $\mathrm{P} \in \mathrm{I}$ arbitraire. Comme A est euclidien, il existe $\mathrm{Q}, \mathrm{R} \in \mathrm{A}$ tels que

$$\mathrm{P} = \mathrm{P}_0\mathrm{Q} + \mathrm{R},$$

et $\mathrm{R} = 0$ ou bien $\rho(\mathrm{R}) < \rho(\mathrm{P}_0) = d$. Or $\mathrm{R} = \mathrm{P} - \mathrm{P}_0\mathrm{Q}$ appartient à I, donc la seconde possibilité est exclue par minimalité de d. Donc $\mathrm{R} = 0$ et $\mathrm{P} = \mathrm{P}_0\mathrm{Q}$. Ceci montre que I est engendré par P_0. La proposition est démontrée. □

Exemple 11.35. — L'anneau $\mathbb{Z}$, muni de la division euclidienne usuelle, est euclidien (l'application $\rho : \mathbb{Z} \to \mathbb{N}$ étant la valeur absolue). On retrouve ainsi que, pour tout idéal $\mathrm{I} \neq (0)$ de $\mathbb{Z}$, on a $\mathrm{I} = (d)$ où d est le plus petit entier > 0 contenu dans I.

Théorème 11.36 **(Division euclidienne dans** $k[\mathrm{X}]$**).** — *Soit* k *un corps.*

1) $k[\mathrm{X}]$ *est intègre et, pour tout* $\mathrm{U} \in k[\mathrm{X}] \setminus \{0\}$*, on peut faire la division euclidienne par* U.

2) *Tout idéal de* $k[\mathrm{X}]$ *est* **principal***, c.-à-d., engendré par un élément. Plus précisément, soit* I *un idéal non nul de* $k[\mathrm{X}]$ *et soit* $\mathrm{U} \in \mathrm{I}$ *un polynôme de degré minimal. Alors* $\mathrm{I} = (\mathrm{U})$*. En particulier,* $k[\mathrm{X}]$ *est noethérien.*

3) $k[\mathrm{X}]$ *est un anneau factoriel.*

Démonstration. — Tout cela résulte de ce qui précède. □

11.6. Exemples d'anneaux noethériens non factoriels. —

Définition 11.37 **(Extensions quadratiques et normes)**. — Soit $n \in \mathbb{Z}$, distinct de 1 et sans facteur carré (c.-à-d., $n = -1$ ou bien $\pm n$ est un produit de nombres premiers > 0 deux à deux distincts). Désignant par $\sqrt{n}$ l'une quelconque des racines carrées de n dans $\mathbb{C}$, considérons le sous-anneau de $\mathbb{C}$ suivant :

$$\mathbb{Z}[\sqrt{n}\,] = \{a + \sqrt{n}\,b \mid a, b \in \mathbb{Z}\}.$$

On a :

$$(a + \sqrt{n}\,b)(a' + \sqrt{n}\,b') = (aa' + nbb') + \sqrt{n}\,(ab' + ba'). \tag{1}$$

Pour $u = a + \sqrt{n}\,b$, on définit son **conjugué** $\overline{u} = a - \sqrt{n}\,b$ et sa **norme** :

$$\mathrm{N}(u) = u\overline{u} = a^2 - nb^2. \tag{2}$$

On déduit de (1) que

$$\overline{uv} = \overline{u}\,\overline{v} \qquad \text{et} \qquad \mathrm{N}(uv) = \mathrm{N}(u)\mathrm{N}(v). \tag{3}$$

Il en résulte que u est inversible si et seulement si $\mathrm{N}(u) = \pm 1$.

Comme $\mathbb{Z}[\sqrt{n}\,]$ est noethérien, tout élément non nul et non inversible de $\mathbb{Z}[\sqrt{n}\,]$ est produit d'éléments irréductibles. Par contre, le Lemme d'Euclide, et l'unicité des facteurs irréductibles, peuvent être en défaut. C'est le cas, par exemple, pour $n = -3, -5$, ou 5.

Exemples 11.38. — 1) Dans $\mathbb{Z}[\sqrt{-3}\,]$, on a $\mathrm{N}(a + \sqrt{-3}\,b) = a^2 + 3b^2$ donc les inversibles sont ± 1 et il n'y a pas d'élément de norme 2. D'autre part, on a l'égalité suivante :

$$2 \cdot 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Tous les facteurs sont de norme 4, donc irréductibles (car il n'y a pas d'élément de norme 2). Si $1 + \sqrt{-3}$ vérifiait le Lemme d'Euclide, il diviserait 2, et comme ce dernier est irréductible, on aurait $2 = u(1 + \sqrt{-3}\,)$, avec u inversible, donc $u = \pm 1$, une contradiction. Ceci montre que $\mathbb{Z}[\sqrt{-3}\,]$ n'est pas factoriel.

2) De même, dans $\mathbb{Z}[\sqrt{-5}\,]$, $\mathrm{N}(a + \sqrt{-5}\,b) = a^2 + 5b^2$ donc les inversibles sont ± 1 et il n'y a pas d'élément de norme 2 ou 3. D'autre part, on a l'égalité

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Les facteurs sont de norme, respectivement, $4, 9, 6, 6$, donc sont irréductibles. Le même argument que précédemment montre que si $1 + \sqrt{-5}$ vérifiait le Lemme d'Euclide, il serait égal à ± 2 ou ± 3, ce qui n'est pas le cas. Ceci montre que $\mathbb{Z}[\sqrt{-5}\,]$ n'est pas factoriel.

3) Dans $\mathbb{Z}[\sqrt{5}\,]$, on a $\mathrm{N}(a + \sqrt{5}\,b) = a^2 - 5b^2$. Il n'y a pas d'élément de norme ± 2. En effet, une égalité $a^2 = \pm 2 + 5b^2$ est impossible, puisque le carré d'un nombre pair (resp. impair) est congru à 0 (resp. 1) modulo 4.

D'autre part, on a l'égalité

$$(1 + \sqrt{5}\,)(-1 + \sqrt{5}\,) = 2 \cdot 2.$$

Les facteurs de gauche sont de norme -4, ceux de droite de norme 4, donc chaque facteur est irréductible, puisqu'il n'y a pas d'élément de norme ± 2. L'élément irréductible 2 ne vérifie pas le Lemme d'Euclide, car sinon on aurait, disons, $1 + \sqrt{5} = 2u$, et

$$u = \frac{1}{2} + \frac{1}{2}\sqrt{5}$$

appartiendrait à $\mathbb{Z}[\sqrt{5}\,]$, ce qui n'est pas le cas, puisque 1 et $\sqrt{5}$ sont linéairement indépendants sur $\mathbb{Q}$. Ceci montre que $\mathbb{Z}[\sqrt{5}\,]$ n'est pas factoriel.

4) Il faut se garder de croire que l'argument précédent s'applique à $\mathbb{Z}[\sqrt{7}\,]$. Dans cet anneau, on a bien l'égalité

$$2 \cdot 3 = 6 = (1 + \sqrt{7}\,)(-1 + \sqrt{7}\,),$$

mais aucun des facteurs ci-dessus n'est irréductible. En effet, on a

$$\begin{array}{ll} 2 = (3 + \sqrt{7}\,)(3 - \sqrt{7}\,), & 1 + \sqrt{7} = (3 + \sqrt{7}\,)(-2 + \sqrt{7}\,), \\ 3 = (2 + \sqrt{7}\,)(-2 + \sqrt{7}\,), & -1 + \sqrt{7} = (3 - \sqrt{7}\,)(2 + \sqrt{7}\,). \end{array}$$

En fait, on peut montrer que $\mathbb{Z}[\sqrt{7}\,]$ est un anneau factoriel, mais la démonstration nécessite des techniques plus sophistiquées, voir par exemple [**Sa**, Ex.V.7].

TABLE DES MATIÈRES

Bibliographie

[Art] E. Artin, Galois Theory, nouvelle édition, Dover, 1998.

[AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.

[BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[ChL] A. Chambert-Loir, Algèbre corporelle, Presses de l'École polytechnique, 2005.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes (2 tomes), Cedic Fernand Nathan, 1977, 2ème éd., Cassini, 2005.

[Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Ja2] N. Jacobson, Basic algebra II, W. H. Freeman & Co., 1980.

[La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : Algèbre, Dunod, 2004.

[Ne04] J. Nekovàř, Théorie de Galois, cours UPMC 2003/4, disponible à l'adresse : www.math.jussieu.fr/~nekovar/co/ln

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[Se] J.-P. Serre, Représentations linéaires des groupes finis, (3ème édition corrigée), Hermann, 1978.

[Ti] J.-P. Tignol, Galois' Theory of algebraic equations, World Scientific, 2001.