V. EXTENSIONS ALGÉBRIQUES, THÉORÈME DES ZÉROS

SEMAINE DU 8 OCTOBRE

Le but de ce chapitre est, d'une part, de commencer l'étude des extensions de corps et, d'autre part, de démontrer le théorème des zéros de Hilbert sur le corps $\mathbb{C}$ des nombres complexes.

10. Extensions de corps

10.1. Généralités sur les extensions de corps. — Commençons par la remarque suivante, facile mais importante.

Remarque 10.1. — Soient K et K′ deux corps et soit $\phi : \mathrm{K} \to \mathrm{K}'$ un morphisme d'anneaux. Alors :

a) ϕ est **injectif**. En effet, $\operatorname{Ker}\phi$, étant un idéal propre de K (puisque $\phi(1) = 1$), est nécessairement nul.

b) ϕ est un **morphisme de corps**, car l'égalité

$$1 = \phi(1) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$$

entraîne que $\phi(x^{-1}) = \phi(x)^{-1}$ pour tout $x \in \mathrm{K} \setminus \{0\}$.

Définition 10.2. — 1) On dit que K est une **extension** de k si l'on s'est donné un morphisme (nécessairement injectif) $k \to \mathrm{K}$. On utilise la notation « K/k » pour signifier que K est une extension de k (il est sous-entendu que k et K sont des corps). Parfois, on dira aussi que K est un **surcorps** de k.

2) Si K/k est une extension, une **extension intermédiaire** L est un corps L tel que $k \subseteq \mathrm{L} \subseteq \mathrm{K}$. Dans ce cas, on dit aussi que L/k est une **sous-extension** de K/k.

Lemme 10.3. — *Soit* K *un corps. Si* $(\mathrm{K}_i)_{i\in\mathrm{I}}$ *est une famille de sous-corps de* K*, alors l'intersection des* K_i *est un sous-corps de* K.

Démonstration. — Facile, et laissée au lecteur. □

***Définition 10.4* (Sous-corps engendré).** — 1) Soient K un corps et S une partie de K. L'ensemble des sous-corps de K contenant S est non-vide (car il contient K) et donc l'intersection de tous ces sous-corps est un sous-corps de K. C'est le plus petit sous-corps contenant S ; on l'appelle le sous-corps **engendré par** S.

2) On appelle **sous-corps premier** de K le sous-corps de K engendré par l'élément 1_{K}. Il est contenu dans tout sous-corps de K.

3) Soit K/k une extension de corps et soit S une partie de K. L'ensemble des sous-corps de K contenant k et S est non-vide (car il contient K) et donc l'intersection de tous ces sous-corps est un sous-corps de K, qui est le plus petit sous-corps contenant k et S. On l'appelle le sous-corps **engendré par** S **sur** k et on le note $k(\mathrm{S})$, ou $k(x_1, \ldots, x_n)$ si $\mathrm{S} = \{x_1, \ldots, x_n\}$.

***Définition 10.5* (Extensions de type fini).** — 1) On dit que K/k est une **extension de type fini** si K est engendré comme surcorps de k par un nombre fini d'éléments, c.-à-d., s'il existe $x_1, \ldots, x_n \in \mathrm{K}$ tels que $\mathrm{K} = k(x_1, \ldots, x_n)$.

2) On dit que K/k est une **extension monogène** si K est engendré sur k par un élément x, c.-à-d., s'il existe $x \in \mathrm{K}$ tel que $\mathrm{K} = k(x)$.

Lemme 10.6. — *Soit* K *un surcorps de* k *et soient* I, J *deux parties de* K. *Alors*

$$k(\mathrm{I} \cup \mathrm{J}) = k(\mathrm{I})(\mathrm{J}).$$

Par conséquent, toute extension de type fini $k \subset k(x_1, \ldots, x_n)$ *est obtenue comme composée d'extensions monogènes :*

$$k(x_1, \ldots, x_n) = k(x_1)(x_2, \ldots, x_n) = k(x_1)(x_2) \cdots (x_n).$$

Démonstration. — $k(\mathrm{I})(\mathrm{J})$ contient $\mathrm{I} \cup \mathrm{J}$ et donc $k(\mathrm{I} \cup \mathrm{J})$. Réciproquement, $k(\mathrm{I} \cup \mathrm{J})$ contient $k(\mathrm{I})$ et J, donc $k(\mathrm{I})(\mathrm{J})$. Ceci prouve le lemme. □

Remarque 10.7. — Dans ce cours, on ne considèrera que des extensions de type fini. Mais les extensions de type infini existent dans la nature. Par exemple, on peut montrer que l'extension $\mathbb{Q} \subseteq \mathbb{R}$ n'est pas de type fini.

***Définition 10.8* (Extensions isomorphes).** — Soient K et K′ deux extensions de k. On dit que K et K′ sont **k-isomorphes** s'il existe un isomorphisme $\phi : \mathrm{K} \xrightarrow{\sim} \mathrm{K}'$ (de corps ou d'anneaux ; on a vu que c'était la même chose) tel que $\phi(\lambda) = \lambda$ pour tout $\lambda \in k$. Ceci équivaut à dire que ϕ est un isomorphisme de k-algèbres.

Plus généralement, si, plutôt qu'une inclusion de k dans K et K′, on s'est donné des morphismes de corps

$$\tau : k \hookrightarrow \mathrm{K} \qquad \text{et} \qquad \tau' : k \hookrightarrow \mathrm{K}',$$

alors un **k-morphisme** de K vers K′ est un morphisme $\phi : \mathrm{K} \to \mathrm{K}'$ tel que $\phi \circ \tau = \tau'$.

10.2. L'alternative algébrique/transcendant. — Soit $k \subset \mathrm{K}$ une extension de corps. Soient $\alpha \in \mathrm{K} \setminus \{0\}$ et $\phi_\alpha : k[\mathrm{X}] \to \mathrm{K}$ le morphisme de k-algèbres défini par $\phi_\alpha(\mathrm{X}) = \alpha$. On pose $\mathrm{I}_\alpha = \operatorname{Ker} \phi_\alpha$.

Notation 10.9. — On note $k[\alpha]$ la **sous-k-algèbre** de K engendrée par α. Alors

$$\phi_\alpha(\mathrm{P}) = \mathrm{P}(\alpha) \in \mathrm{K}, \qquad \forall\, \mathrm{P} \in k[\mathrm{X}],$$

et l'image de ϕ_α est $k[\alpha]$.

Puisque $k[\mathrm{X}]/\mathrm{I}_\alpha \cong k[\alpha]$ est *intègre*, alors I_α est un idéal premier de $k[\mathrm{X}]$. Donc, d'après les théorèmes 9.30 et 9.26, de deux choses l'une : ou bien $\mathrm{I}_\alpha = (0)$ ou bien $\mathrm{I}_\alpha = (\mathrm{P})$ pour un polynôme irréductible (uniquement déterminé si on le suppose unitaire). Ceci conduit à l'alternative suivante.

Définition 10.10 **(Éléments transcendants ou algébriques)**

1) Si $\mathrm{I}_\alpha = (0)$, on dit que α est **transcendant** sur k.

2) Si $\mathrm{I}_\alpha \neq (0)$, on dit que α est **algébrique** sur k. Dans ce cas, $\mathrm{I}_\alpha = (\mathrm{P})$, où P est l'unique polynôme unitaire de degré minimal dans I_α ; il est appelé **polynôme minimal de α sur k**. On le notera $\mathrm{Irr}_k(\alpha)$. Son degré s'appelle **degré de α sur k** et se note $\deg_k(\alpha)$.

Théorème 10.11 **(Extensions monogènes $k(x)$)**. — *Supposons* $\mathrm{K} = k(x)$.

1) *Si x est algébrique sur k, alors $k(x)$ coïncide avec la sous-algèbre $k[x]$. Plus précisément,* $\mathrm{Irr}_k(x)$ *est irréductible et l'on a*

$$(*) \qquad k[\mathrm{X}]/(\mathrm{Irr}_k(x)) \xrightarrow{\sim} k[x] = k(x).$$

Par conséquent, les éléments $1, x, \ldots, x^{d-1}$*, où* $d = \deg_k(x)$*, forment une base de $k(x)$ sur k. En particulier,* $\dim_k k(x) = d$.

2) *Si x est transcendant sur k, alors l'injection $\phi_x : k[\mathrm{X}] \hookrightarrow \mathrm{K} = k(x)$ induit un k-isomorphisme $k(\mathrm{X}) \xrightarrow{\sim} k(x)$. En particulier,* $\dim_k k(x) = +\infty$.

Démonstration. — 1) $k[\mathrm{X}]/\mathrm{I}_x$ est intègre car isomorphe à $k[x]$, la sous-k-algèbre de K engendrée par x. Ainsi, $\mathrm{I}_x = (\mathrm{Irr}_k(x))$ est un idéal premier non nul. Donc, d'après le théorème 9.26, $\mathrm{Irr}_k(x)$ est irréductible et engendre un idéal maximal de $k[\mathrm{X}]$. Donc, $\mathrm{A} := k[\mathrm{X}]/(\mathrm{Irr}_k(x))$ est un corps.

Par conséquent, son image par ϕ_x, qui est $k[x]$, égale le corps $k(x)$ engendré par x. Ceci prouve $(*)$. Comme les images de $1, \ldots, \mathrm{X}^{d-1}$ forment une base de A sur k, la dernière assertion de 1) en découle.

2) Supposons x transcendant, c.-à-d., $\phi_x : k[\mathrm{X}] \hookrightarrow \mathrm{K} = k(x)$ injectif. Alors, tout élément de $\phi_x(k[\mathrm{X}] \setminus \{0\})$ est inversible dans K. Donc, d'après la propriété universelle du corps des fractions (Proposition 9.35), ϕ_x se prolonge (de façon unique) en un morphisme d'anneaux $\psi : k(\mathrm{X}) \to \mathrm{K}$; injectif puisque $k(\mathrm{X})$

est un corps, et surjectif puisque K est engendré sur k par x. Donc ψ est un isomorphisme $k(\mathrm{X}) \xrightarrow{\sim} k(x) = \mathrm{K}$. De plus, on a un diagramme commutatif

$$\begin{array}{ccc} k[\mathrm{X}] & \hookrightarrow & k(\mathrm{X}) \\ \cong\downarrow & & \downarrow\cong \\ k[\alpha] & \hookrightarrow & k(\alpha) \end{array}$$

où les flèches verticales sont des isomorphismes, et les inclusions sont des inclusions strictes (car $k[\mathrm{X}] \neq k(\mathrm{X})$). Donc, dans ce cas, on a $k[\alpha] \neq k(\alpha)$.

D'autre part, les monômes X^i, $i \in \mathbb{N}$, forment une k-base de $k[\mathrm{X}]$, donc $k[\mathrm{X}]$ (et de même $k[\alpha]$, pour α transcendant), est de dimension infinie mais dénombrable sur k. A fortiori, $\dim_k k(\mathrm{X}) = +\infty$ (et on verra plus loin que cette dimension est non dénombrable si k est non dénombrable). □

Remarques 10.3. — 1) Dans le cas où x est algébrique (et $\neq 0$), écrivons $\mathrm{Irr}_k(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$. Alors

$$x(x^{d-1} + a_{d-1}x^{d-2} + \cdots + a_1) = a_0$$

et nécessairement $a_0 \neq 0$, puisque le terme de gauche est non nul (car $x^{d-1} + \cdots + a_1$ ne divise pas $\mathrm{Irr}_k(x)$). Donc l'inverse de x est égal à

$$(x^{d-1} + a_{d-1}x^{d-2} + \cdots + a_1)a_0^{-1}.$$

2) Dans le cas où x est transcendant et k infini, l'égalité $\dim_k k(x) = +\infty$ sera précisée plus loin en l'inégalité $\dim_k k(x) \geqslant \mathrm{card}(k)$; en particulier, si k est non dénombrable (par exemple $k = \mathbb{C}$), alors $k(x)$ est de dimension non dénombrable sur k.

Remarque 10.12. — Soit L un corps intermédiaire entre k et K, c.-à-d., $k \subseteq \mathrm{L} \subseteq \mathrm{K}$. Si $\alpha \in k$ est algébrique sur k, il l'est aussi sur L et $\mathrm{Irr}_k(\alpha)$ est divisible, dans $\mathrm{L}[\mathrm{X}]$, par $\mathrm{Irr}_{\mathrm{L}}(\alpha)$.

10.4. Extensions algébriques et degré. — On vient de voir que si $\mathrm{K} = k(x)$, où x est un élément algébrique sur k, alors $\dim_k \mathrm{K} = \deg_k(x)$. Ceci explique la terminologie suivante.

Définition 10.13. — Soit K/k une extension de corps. Alors, K est un k-espace vectoriel et $\dim_k \mathrm{K}$ s'appelle **degré de** K **sur** k et se note $[\mathrm{K} : k]$. C'est un élément de $\mathbb{N}^* \cup \{+\infty\}$.

Proposition 10.14 **(Multiplicativité des degrés)**. — *Soient* $k \subset \mathrm{K} \subset \mathrm{L}$ *des extensions de corps. Alors* $[\mathrm{L} : k] = [\mathrm{L} : \mathrm{K}]\,[\mathrm{K} : k]$.

Démonstration. — Montrons d'abord que si l'un des termes de droite égale $+\infty$, alors $[\mathrm{L} : k] = +\infty$. Prenant la contraposée, ceci équivaut à montrer que si $[\mathrm{L} : k]$ est fini, il en est de même de $[\mathrm{L} : \mathrm{K}]$ et $[\mathrm{K} : k]$. Supposons donc que $[\mathrm{L} : k] = \mathrm{N} < +\infty$. Comme K est un sous-$k$-espace vectoriel de L, on a

$$[\mathrm{K} : k] \leqslant [\mathrm{L} : k] = \mathrm{N}.$$

D'autre part, si $(y_1, \ldots, y_\mathrm{N})$ est une base de L sur k, alors les y_i engendrent *a fortiori* L comme K-espace vectoriel, et donc $[\mathrm{L} : \mathrm{K}] \leqslant [\mathrm{L} : k] = \mathrm{N}$.

Pour démontrer la proposition, on peut donc supposer que $[\mathrm{L} : \mathrm{K}] = m$ et $[\mathrm{K} : k] = n$, et il s'agit de montrer que

$$[\mathrm{L} : k] = mn.$$

Donnons deux démonstrations.

1) Comme k-espace vectoriel, K est isomorphe à k^n et, comme K-espace vectoriel, L est isomorphe à K^m. Donc, comme k-espace vectoriel, L est isomorphe à :

$$\underbrace{\mathrm{K} \oplus \cdots \oplus \mathrm{K}}_{m \text{ facteurs}} \cong \underbrace{k^n \oplus \cdots \oplus k^n}_{m \text{ facteurs}} \cong k^{mn},$$

d'où $\dim_k \mathrm{L} = mn$, ce qui prouve la proposition.

2) De façon plus explicite, soient $(\ell_1, \ldots, \ell_m)$ une base de L sur K et $(x_1, \ldots, x_n)$ une base de K sur k. Alors, on voit facilement que les produits $x_i \ell_j$ engendrent L comme k-espace vectoriel, voir par exemple la preuve du lemme 10.16 qui suit. Montrons que ces éléments sont linéairement indépendants sur k. Supposons qu'on ait une égalité

$$0 = \sum_{i,j} a_{i,j}\, x_i \ell_j,$$

avec les $a_{i,j} \in k$. Alors on a

$$0 = \sum_{1 \leqslant i \leqslant m} \left(\sum_{1 \leqslant j \leqslant n} a_{i,j}\, x_j \right) \ell_i.$$

Comme les ℓ_i sont linéairement indépendants sur K, on obtient que, pour tout $i = 1, \ldots, m$,

$$\sum_{1 \leqslant j \leqslant n} a_{i,j}\, x_j = 0.$$

Puis, comme les x_j sont linéairement indépendants sur k, on obtient que $a_{i,j} = 0$ pour tout i, j. Ceci montre que les produits $x_j \ell_i$ forment une base de L sur k, d'où $\dim_k \mathrm{L} = mn$. □

Remarque 10.15. — La même démonstration montre que si $\mathrm{A} \subset \mathrm{B}$ sont deux anneaux, et si $\mathrm{B} \cong \mathrm{A}^n$ comme A-module, alors, pour tout $r \geqslant 1$, B^r est libre comme A-module, de rang rn. Le lemme cité dans la démonstration est le suivant.

Lemme 10.16. — *Soient* $\mathrm{A} \subset \mathrm{B}$ *des anneaux et* N *un* B*-module de type fini. On suppose que* B *est un* A*-module de type fini. Alors* N *est un* A*-module de type fini.*

Démonstration. — Par hypothèse, il existe des éléments $x_1, \ldots, x_r$ dans N (resp. $b_1, \ldots, b_n$ dans B) qui engendrent N comme B-module (resp. B comme A-module). Alors

$$\mathrm{N} = \mathrm{B}x_1 + \cdots + \mathrm{B}x_r$$

et chaque $\mathrm{B}x_j$ est engendré, comme A-module, par les éléments $b_i x_j$. Il en résulte que N est engendré comme A-module par les éléments $b_i x_j$. Ceci prouve le lemme. □

Définition 10.17. — Soit $k \subset \mathrm{K}$ une extension de corps. On dit que K/k est une extension **algébrique** si tout élément de K est algébrique sur k.

Lemme 10.18. — *Pour* $\lambda \in k$*, les éléments* $1/(\mathrm{X}-\lambda)$ *de* $k(\mathrm{X})$ *sont linéairement indépendants.*

Démonstration. — Supposons qu'on ait une relation de dépendance linéaire

$$0 = \sum_{j=1}^{n} \frac{a_j}{\mathrm{X} - \lambda_j}.$$

Alors, multipliant par $\prod_{j=1}^{n}(\mathrm{X} - \lambda_j)$ puis évaluant en $\mathrm{X} = \lambda_i$, on trouve

$$0 = a_i \prod_{j \neq i} (\lambda_i - \lambda_j),$$

d'où $a_i = 0$. □

Corollaire 10.19. — *Supposons* k *non dénombrable (par exemple,* $k = \mathbb{R}$ *ou* $\mathbb{C}$*). Soit* $\mathfrak{m}$ *un idéal maximal de* $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$*. Alors le corps*

$$\mathrm{K} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathfrak{m}$$

est algébrique sur k*.*

Démonstration. — Comme k-espace vectoriel, $\mathrm{A} := k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est de dimension dénombrable (car il admet la base des monômes X^ν, $\nu \in \mathbb{N}^n$), donc il en est de même du quotient $\mathrm{K} = \mathrm{A}/\mathfrak{m}$. (Noter que le morphisme composé $\phi : k \hookrightarrow \mathrm{A} \to \mathrm{K}$ est non nul, car $\phi(1) = 1$, donc K est une extension de k.)

Si K contenait un élément x transcendant sur k, alors $\dim_k \mathrm{K} \geqslant \dim_k k(x)$ serait non dénombrable, d'après le lemme précédent. Donc K est algébrique sur k. □

10.5. Corps algébriquement clos. —

Définition 10.20. — Soit $k \subseteq \mathrm{K}$ une extension de corps et soit $\mathrm{P} \in k[\mathrm{X}]$ non constant. On dit que P est **scindé dans** K[X], ou **sur** K, si P se décompose *dans* K[X] comme produit de facteurs du premier degré, c.-à-d., si

$$\mathrm{P} = c(\mathrm{X} - \alpha_1) \cdots (\mathrm{X} - \alpha_d),$$

où $d = \deg \mathrm{P}$, c est le coefficient dominant de P, et les α_i sont dans K (pas nécessairement distincts).

Définition 10.21. — Un corps k est dit **algébriquement clos** si tout $\mathrm{P} \in k[\mathrm{X}]$ non constant a au moins une racine dans K.

Proposition 10.22. — *Supposons k algébriquement clos. Alors :*

1) *Tout* $\mathrm{P} \in k[\mathrm{X}]$ *non constant est scindé. En particulier, si* P *est irréductible, il est de degré* 1.

2) *Soit* K/k *une extension algébrique. Alors* $\mathrm{K} = k$.

Démonstration. — Montrons 1) par récurrence sur $d = \deg \mathrm{P}$. C'est clair si $d = 1$. Supposons $d \geqslant 2$ et l'assertion établie en degré $< d$. Soit $\mathrm{P} \in k[\mathrm{X}]$ de degré d. Comme k est algébriquement clos, P possède dans k au moins un racine α, donc se factorise en $\mathrm{P} = (\mathrm{X} - \alpha)\mathrm{Q}$, avec $\mathrm{Q} \in k[\mathrm{X}]$ de degré $d-1$. Par hypothèse de récurrence, Q est scindé dans $k[\mathrm{X}]$, et donc il en est de même de P.

2) Soit K/k une extension algébrique et soit $x \in \mathrm{K}$. Le polynôme minimal $\mathrm{Irr}_k(x)$ est irréductible (cf. 10.11), donc de degré 1, c.-à-d., de la forme $\mathrm{X} - a$, avec $a \in k$. Donc x égale a et appartient à k. Ceci prouve 2). La proposition est démontrée. □

Définition 10.23. — Soit $k \subseteq \mathrm{K}$ une extension de corps. On dit que K est une **clôture algébrique de** k si K est algébriquement clos et si tout élément de K est algébrique sur k.

10.6. $\mathbb{C}$ est algébriquement clos. —

Théorème 10.24. — $\mathbb{C}$ *est algébriquement clos, c.-à-d., tout polynôme* $\mathrm{P} \in \mathbb{C}[\mathrm{X}]$*, non constant, admet une racine dans* $\mathbb{C}$.

Ce résultat est parfois appelé, surtout dans la littérature anglaise, « Théorème fondamental de l'algèbre ». Dans la littérature française, il est souvent appelé « Théorème de d'Alembert ». L'auteur de ces notes n'est pas compétent quant à la question de savoir si la preuve proposée par d'Alembert était complète dans tous ses détails. Quatre autres preuves ont été proposées par Gauss, dont l'une au moins était tout-à-fait complète (mais longue et compliquée), voir par exemple le livre de van der Waerden [**vdW**].

Nous allons donner une démonstration qui n'utilise que des méthodes élémentaires d'analyse ; elle est attribuée à Argand, en 1814 (voir [**Esc**, p.5]), bien que la notion de compacité, utilisée pour assurer que le minimum est atteint, n'ait été dégagée que dans la deuxième moitié du 19e siècle (entre autre, par Weierstrass). Bref, les premières preuves simples et complètes de ce théorème datent probablement des années 1850 ou 1860. Pour une autre démonstration, plus algébrique (et un peu moins élémentaire), voir [**Sa**, Chap.II, Appendice].

La démonstration d'Argand. — Soit $\mathrm{P} \in \mathbb{C}[\mathrm{X}]$ un polynôme de degré $n \geqslant 1$. Sans perte de généralité, on peut supposer P *unitaire*, c.-à-d., de coefficient dominant égal à 1. Écrivons

$$\mathrm{P} = \mathrm{X}^n + a_1\mathrm{X}^{n-1} + \cdots + a_n.$$

Raisonnons par l'absurde et supposons que P ne s'annule pas sur $\mathbb{C}$. Alors, en particulier, $a_n \neq 0$. Notons $|\cdot|$ la norme usuelle sur $\mathbb{C}$, c.-à-d., si $z = x + iy$ alors

$$|z| = \sqrt{z\overline{z}} = \sqrt{x^2 + y^2}.$$

Comme $\lim_{|z|\to+\infty} |\mathrm{P}(z)| = +\infty$, il existe $\mathrm{R} > 0$ tel que

$$|z| \geqslant \mathrm{R} \Rightarrow |\mathrm{P}(z)| \geqslant |a_n|. \tag{1}$$

Explicitement, on peut prendre $\mathrm{R} = \max\{1, 2na\}$, où $a = \max_{i=1}^n |a_i|$. En effet, pour $|z| \geqslant \mathrm{R}$ et $d = 1, \ldots, n$, on a $|z^d| \geqslant |z| \geqslant 2na$ d'où

$$\left|\sum_{d=1}^{n} \frac{a_d}{z^d}\right| \leqslant \sum_{d=1}^{n} \frac{|a_d|}{2na} \leqslant \frac{1}{2}.$$

Comme $|u + v| \geqslant |u| - |v|$, on obtient que, pour $|z| \geqslant \mathrm{R}$, on a

$$|\mathrm{P}(z)| = |z^n| \cdot \left|1 + \sum_{d=1}^{n} \frac{a_d}{z^d}\right| \geqslant 2na(1 - \frac{1}{2}) = na \geqslant n|a_n|.$$

Comme le disque D de centre 0 et de rayon R est compact, la fonction continue $f : z \mapsto |\mathrm{P}(z)|$ y atteint son minimum r_0, et $r_0 > 0$ puisqu'on a supposé que P ne s'annule pas. Comme de plus

$$r_0 \leqslant |\mathrm{P}(0)| = |a_n| \leqslant f(z), \quad \forall\, z \notin \mathrm{D}, \tag{2}$$

alors r_0 est le minimum de f sur $\mathbb{C}$ tout entier.

Soit $z_0 \in \mathrm{D}$ tel que $f(z_0) = r_0$. En remplaçant z par $z + z_0$ et $\mathrm{P}(z)$ par $\mathrm{Q}(z) := \mathrm{P}(z_0)^{-1}\mathrm{P}(z + z_0)$, on se ramène au cas où $z_0 = 0$ et où $\mathrm{Q}(0) = 1$ est le minimum de $g = |\mathrm{Q}|$ sur $\mathbb{C}$.

Observons que Q est, comme P, de degré n. Notons k l'ordre d'annulation en 0 de $\mathrm{Q} - 1$. On peut alors écrire

$$\mathrm{Q}(\mathrm{X}) = 1 + b_k\mathrm{X}^k + \cdots + b_n\mathrm{X}^n.$$

avec $b_k b_n \neq 0$. Écrivons $b_k = re^{i\theta}$, avec $r > 0$ et $\theta \in [0, 2\pi[$ et, pour $\varepsilon \in \mathbb{R}_+^*$, posons

$$z_\varepsilon = \varepsilon e^{i(\pi-\theta)/k}, \quad \text{et} \quad q(\varepsilon) = \mathrm{Q}(z_\varepsilon).$$

Comme $z_\varepsilon^k = \varepsilon^k\, e^{i(\pi-\theta)}$ et $e^{i\pi} = -1$, alors

$$q(\varepsilon) = 1 - r\varepsilon^k + \varepsilon^k h(\varepsilon),$$

où $h(\varepsilon) = \sum_{j=1}^{n-k} b_{k+j} z_\varepsilon^j$. Comme $\lim_{\varepsilon\to 0} \varepsilon^k = 0$ et $\lim_{\varepsilon\to 0} h(\varepsilon) = 0$, il existe $\varepsilon_0 \in]0, 1[$ tel que

$$\forall\, \varepsilon \leqslant \varepsilon_0, \qquad r\varepsilon^k < 1 \quad \text{et} \quad |h(\varepsilon)| \leqslant \frac{r}{2}.$$

On a alors

$$|\mathrm{Q}(z_{\varepsilon_0})| = |1 - r\varepsilon_0^k + \varepsilon_0^k h(\varepsilon_0)| \leqslant 1 - r\varepsilon_0^k + \frac{r}{2}\varepsilon_0^k = 1 - \frac{r}{2}\varepsilon_0^k < 1.$$

Ceci contredit l'hypothèse que $1 = \mathrm{Q}(0)$ était le minimum de $g = |\mathrm{Q}|$ sur $\mathbb{C}$. Cette contradiction montre que l'hypothèse que P ne s'annule pas sur $\mathbb{C}$ est impossible. Ceci achève la démonstration du théorème. □

11. Le théorème des zéros de Hilbert

11.1. Idéaux maximaux de $\mathbb{C}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. — Pour le moment, soit k un corps arbitraire.

Remarque 11.1. — Un polynôme $\mathrm{P} = \sum_{\nu\in\mathbb{N}^n} a_\nu \mathrm{X}^\nu$ s'annule au point $0 = (0, \ldots, 0)$ de k^n si, et seulement si, son coefficient constant a_0 est nul.

Soit $x = (x_1, \ldots, x_n)$ un élément arbitraire de k^n. Par le changement de variable $\mathrm{X}_i \to \mathrm{X}_i - x_i$, on peut écrire tout polynôme P comme une constante plus une somme de monômes en les $\mathrm{X}_i - x_i$ de degré > 0, le terme constant valant dans ce cas $\mathrm{P}(x)$.

***Définition 11.2* (Les idéaux $\mathfrak{m}_x$, pour $x \in k^n$).** — Pour tout $x \in k^n$, notons $\mathfrak{m}_x$ l'idéal engendré par $\mathrm{X}_1 - x_1, \ldots, \mathrm{X}_n - x_n$. D'après ce qui précède, c'est le noyau du morphisme surjectif de k-algèbres suivant (évaluation en x) :

$$\varepsilon_x : k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \longrightarrow k, \qquad \mathrm{P} \mapsto \mathrm{P}(x).$$

Comme $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathfrak{m}_x \cong k$ est un corps, $\mathfrak{m}_x$ est un idéal maximal de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$.

Pour I un idéal arbitraire de $k[X_1, \dots, X_n]$, on voit que :

$$I \subseteq \mathfrak{m}_x \Leftrightarrow P(x) = 0, \quad \forall P \in I.$$

On pose

$$\mathscr{V}(I) = \{x \in k^n \mid P(x) = 0, \quad \forall P \in I\} = \{x \in k^n \mid I \subseteq \mathfrak{m}_x\};$$

on l'appelle la *variété des zéros* de I.

Alors, on voit facilement que $\mathscr{V}(\mathfrak{m}_x) = \{x\}$; en particulier, les $\mathfrak{m}_x$ sont deux à deux distincts.

***Théorème 11.3* (Théorème des zéros, forme faible).** — *On suppose $k = \mathbb{C}$.*

1) *Soit $\mathfrak{m}$ un idéal maximal de $\mathbb{C}[X_1, \dots, X_n]$. Alors $\mathfrak{m} = \mathfrak{m}_x$, pour un unique $x \in \mathbb{C}^n$.*

2) *Soit J un idéal propre de $\mathbb{C}[X_1, \dots, X_n]$. Alors $\mathscr{V}(J) \neq \varnothing$.*

Démonstration. — 1) Comme $\mathbb{C}$ est non dénombrable et algébriquement clos, le corollaire 10.19 et la proposition 10.22 entraînent que

$$\mathbb{C}[X_1, \dots, X_n]/\mathfrak{m} = \mathbb{C}.$$

Notons π la projection

$$\mathbb{C}[X_1, \dots, X_n] \longrightarrow \mathbb{C}[X_1, \dots, X_n]/\mathfrak{m} = \mathbb{C},$$

et soit $x_i = \pi(X_i)$ l'image de X_i dans $\mathbb{C}$; alors $\mathfrak{m}$ contient les polynômes

$$X_i - x_i \cdot 1, \qquad \forall\, i = 1, \dots, n,$$

car $\pi(X_i - x_i \cdot 1) = x_i - x_i \cdot 1 = 0$. Donc, posant $x = (x_1, \dots, x_n)$, on obtient que $\mathfrak{m}$ contient l'idéal maximal $\mathfrak{m}_x$, d'où $\mathfrak{m} = \mathfrak{m}_x$. Ceci prouve 1).

Soit J un idéal propre. Comme $\mathbb{C}[X_1, \dots, X_n]$ est noethérien (Théorème 8.17), J est contenu dans un idéal maximal $\mathfrak{m}_x$, et donc $\mathscr{V}(J)$ contient x. Le théorème est démontré. □

11.2. Sous-variétés algébriques de $\mathbb{C}^n$. — Pour le moment, soit k un corps arbitraire. On rappelle la définition suivante.

Définition 11.4. — Une **sous-variété algébrique fermée** de k^n est un sous-ensemble de k^n défini par une collection arbitraire d'équations polynomiales, c.-à-d., un sous-ensemble de la forme :

$$\mathscr{V}(S) = \{x \in k^n \mid P(x) = 0, \forall P \in S\},$$

où S est une partie arbitraire de $k[X_1, \dots, X_n]$. Si on note I l'idéal engendré par S, on voit facilement que

$$\mathscr{V}(S) = \mathscr{V}(I) = \mathscr{V}(\sqrt{I}).$$

En particulier, comme tout idéal de $k[X_1, \ldots, X_n]$ est engendré par un nombre fini d'éléments (Théorème 8.17), on voit que toute $\mathscr{V}(S)$ peut être définie par un nombre fini d'équations polynomiales.

Réciproquement, à tout sous-ensemble $V \subseteq k^n$ on associe l'idéal

$$\mathscr{I}(V) = \{\varphi \in k[X_1, \ldots, X_n] \mid \varphi(V) = 0\}.$$

C'est un idéal **réduit** (car si φ^r s'annule sur V, il en est de même de φ), et on voit facilement que $V \subseteq \mathscr{V}(\mathscr{I}(V))$.

D'autre part, les applications $I \mapsto \mathscr{V}(I)$ et $V \mapsto \mathscr{I}(V)$ sont décroissantes, c.-à-d., vérifient :

$$\begin{cases} I \subseteq J \ \Rightarrow \ \mathscr{V}(I) \supseteq \mathscr{V}(J); \\ V \subseteq W \Rightarrow \mathscr{I}(V) \supseteq \mathscr{I}(W). \end{cases} \tag{1}$$

De ceci, on déduit le lemme suivant.

Lemme 11.5. — *$\mathscr{V}(\mathscr{I}(V))$ est la plus petite sous-variété algébrique fermée de k^n contenant V. En particulier, V est une sous-variété algébrique fermée de k^n si et seulement si $V = \mathscr{V}(\mathscr{I}(V))$.*

Démonstration. — En effet, si $V \subseteq \mathscr{V}(J)$ alors J est contenu dans $\mathscr{I}(V)$, d'où $V \subseteq \mathscr{V}(\mathscr{I}(V)) \subseteq \mathscr{V}(J)$. Ceci prouve le lemme. □

Définition 11.6 **(L'algèbre** $k[V]$**)**. — À chaque sous-variété algébrique fermée $V \subseteq k^n$, on associe la k-algèbre réduite

$$k[V] = k[X_1, \ldots, X_n]/\mathscr{I}(V).$$

On l'appelle l'algèbre des fonctions régulières (ou polynomiales) sur V.

Théorème 11.7 **(Théorème des zéros de Hilbert)**. — *On suppose $k = \mathbb{C}$. Soit I un idéal de $\mathbb{C}[X_1, \ldots, X_n]$. Alors $\mathscr{I}(\mathscr{V}(I)) = \sqrt{I}$.*

Démonstration. — Posons $V = \mathscr{V}(I)$. Alors $\mathscr{I}(V)$ est réduit et contient I, donc aussi $\sqrt{I}$. Réciproquement, soit $f \in \mathscr{I}(V)$.

Dans l'anneau de polynômes $\mathbb{C}[X_0, X_1, \ldots, X_n]$ avec une indéterminée supplémentaire X_0, considérons l'idéal J engendré par I et le polynôme $1 - fX_0$. Alors $\mathscr{V}(J) = \varnothing$. En effet, si $x = (x_0, x_1, \ldots, x_n) \in \mathscr{V}(J)$, alors $g(x) = g(x_1, \ldots, x_n) = 0$ pour tout $g \in I$, donc le point $(x_1, \ldots, x_n)$ appartient à $\mathscr{V}(I) \subseteq \mathbb{C}^n$, et donc

$$f(x_1, \ldots, x_n) = 0,$$

puisque $f \in \mathscr{I}(\mathscr{V}(I))$. On obtient donc

$$0 = (1 - fX_0)(x) = 1 - f(x)x_0 = 1,$$

une contradiction. Ceci montre que $\mathscr{V}(J) = \varnothing$.

Par conséquent, d'après le théorème 11.3, on a $J = (1)$. Il existe donc $r \geqslant 1$ et $P_1, \ldots, P_r \in I$, $S_0, \ldots, S_r \in \mathbb{C}[X_0, \ldots, X_n] = \mathbb{C}[X_1, \ldots, X_n][X_0]$ tels que

$$(*) \qquad 1 = S_1P_1 + \cdots + S_rP_r + S_0(1 - fX_0).$$

Notons d_i le degré en X_0 de S_i et $d = \max\{d_1, \ldots, d_r\}$. Considérons le morphisme de $\mathbb{C}[X_1, \ldots, X_n]$-algèbres

$$\phi : \mathbb{C}[X_1, \ldots, X_n][X_0] \longrightarrow \mathbb{C}(X_1, \ldots, X_n)$$

défini par $\phi(X_0) = 1/f$, et appliquons ϕ à l'égalité $(*)$. On obtient ainsi, dans $\mathbb{C}(X_1, \ldots, X_n)$, une égalité de la forme

$$1 = \frac{U_1}{f^d}P_1 + \cdots + \frac{U_r}{f^d}P_r,$$

où chaque $U_i = f^dS_i(1/f, X_1, \ldots, X_n)$ appartient à $\mathbb{C}[X_1, \ldots, X_n]$ (car $d \geqslant d_i = \deg_{X_0} S_i$). Donc, en multipliant par f^d on obtient dans $\mathbb{C}[X_1, \ldots, X_n]$ l'égalité

$$f^d = U_1P_1 + \cdots + U_rP_r,$$

qui montre que $f^d \in I$. Le théorème est démontré. □

On peut maintenant énoncer des conséquences plus géométriques du théorème des zéros. Rappelons la définition et la proposition suivantes, déjà vues aux §§ 9.1 et 9.10.

Définition 11.8. — Une sous-variété algébrique fermée V de $\mathbb{C}^n$ est dite **irréductible** si elle n'est pas réunion de deux fermés algébriques strictement plus petits, c.-à-d., si la propriété suivante est vérifiée : si I, J sont deux idéaux de $\mathbb{C}[X_1, \ldots, X_n]$ tels que $V = V(I) \cup V(J)$, alors $V(I) = V$ ou $V(J) = V$.

Proposition 11.9. — V *est irréductible* $\Leftrightarrow \mathscr{I}(V)$ *est premier.*

Démonstration. — Posons $A = \mathbb{C}[X_1, \ldots, X_n]$. Supposons V irréductible et soient $f, g \in A$ tels que $f \notin \mathscr{I}(V)$ et $fg \in \mathscr{I}(V)$. Posant $I = \mathscr{I}(V) + Af$ et $J = \mathscr{I}(V) + Ag$, on a $V(I) \neq V$ (car sinon on aurait $f \in \mathscr{I}(V)$) et $V = V(I) \cup V(J)$ (car fg est nulle sur V). Comme V est irréductible, il vient $V(J) = V$ et donc $g \in \mathscr{I}(V)$. Ceci montre que $\mathscr{I}(V)$ est premier.

Réciproquement, supposons $\mathscr{I}(V)$ premier. Si V égale $V(I) \cup V(J) = V(IJ)$, alors IJ est contenu dans $\mathscr{I}(V)$ et comme ce dernier est premier, il contient I ou J, et il en résulte que V est contenue dans, donc égale à, $V(I)$ ou $V(J)$. Ceci prouve que V est irréductible. □

Corollaire 11.10. — *Les applications*

$$V \mapsto \mathscr{I}(V) \qquad \textit{et} \qquad I \mapsto \mathscr{V}(I)$$

sont des bijections réciproques entre l'ensemble des sous-variétés algébriques fermées de $\mathbb{C}^n$ *et celui des idéaux réduits de* $\mathbb{C}[X_1, \ldots, X_n]$. *Dans cette correspondance, les sous-variétés irréductibles correspondent aux idéaux premiers, et les points* x *de* $\mathbb{C}^n$ *aux idéaux maximaux* $\mathfrak{m}_x$.

Démonstration. — On a déjà vu la dernière assertion, ainsi que l'égalité $V = \mathscr{V}(\mathscr{I}(V))$. D'autre part, si I est réduit le théorème des zéros entraîne que $I = \mathscr{I}(\mathscr{V}(I))$. Ceci prouve que les deux applications sont inverses l'une de l'autre, et, compte-tenu de la proposition précédente, le corollaire en découle. □

Soit V une sous-variété algébrique fermée de $\mathbb{C}^n$. On lui a associé la $\mathbb{C}$-algèbre réduite $\mathbb{C}[V] := \mathbb{C}[X_1, \ldots, X_n]/\mathscr{I}(V)$. Les points $x \in V$ correspondent exactement aux idéaux maximaux $\mathfrak{m}_x$ qui contiennent $\mathscr{I}(V)$, c.-à-d., aux idéaux maximaux de l'algèbre $\mathbb{C}[V]$. De même, d'après les théorèmes 4.5 et 4.13, les idéaux réduits (resp., premiers) de $\mathbb{C}[V]$ peuvent être identifiés aux idéaux réduits (resp. premiers) de $\mathbb{C}[X_1, \ldots, X_n]$ contenant $\mathscr{I}(V)$. On obtient donc le corollaire suivant.

Corollaire 11.11. — *Soit* V *une sous-variété algébrique fermée de* $\mathbb{C}^n$. *Les idéaux maximaux (resp. premiers) de* $\mathbb{C}[V]$ *correspondent, respectivement, aux points de* V *et aux sous-variétés algébriques fermées de* V.

Remarque 11.12. — Pour d'autres démonstrations du théorème des zéros (valables aussi pour k algébriquement clos dénombrable), ou des compléments, voir, par exemple, [**Elk**, § X.4] [**BM**, Thm. VI.2.19], [**Die**, (A, 37)], ou [**Pe2**, § I.4].

11.3. Composantes irréductibles. —

Théorème 11.13. — *Soient* A *un anneau* **noethérien** *et* I *un idéal propre* **réduit** *de* A. *Il existe un nombre fini d'idéaux premiers* $P_1, \ldots, P_n$ *tels que :*

$$(*) \qquad I = P_1 \bigcap \cdots \bigcap P_n \qquad \textit{et} \quad P_i \not\subseteq P_j \textit{ si } i \neq j.$$

Tout idéal premier contenant I *contient l'un des* P_i, *de sorte que les* P_i *sont exactement les éléments minimaux de l'ensemble*

$$\{P \in \mathrm{Spec}(A) \mid P \supseteq I\};$$

on les appelle les **idéaux premiers minimaux au-dessus de** I.

Démonstration. — Notons $\mathscr{I}$ l'ensemble des idéaux propres réduits de A qui **ne sont pas** intersection finie d'idéaux premiers de A. Il s'agit de montrer que $\mathscr{I} = \varnothing$. Supposons, au contraire, $\mathscr{I} \neq \varnothing$. Alors, comme A est noethérien, $\mathscr{I}$ possède au moins un élément I_0 maximal pour l'inclusion.

Comme $\mathrm{I}_0 \notin \mathscr{I}$, alors I_0 n'est pas premier, donc il existe des idéaux propres J, K contenant *strictement* I_0 et tels que :

$$(\dagger) \qquad \mathrm{JK} \subseteq \mathrm{I}_0 \subseteq \mathrm{J} \cap \mathrm{K}.$$

En effet, prendre $a, b \in \mathrm{A} \setminus \mathrm{I}_0$ tels que $ab \in \mathrm{I}_0$, et $\mathrm{J} = \mathrm{I}_0 + \mathrm{A}a$, $\mathrm{J} = \mathrm{I}_0 + \mathrm{A}b$; ce sont des idéaux *propres* car si on avait, par exemple, $\mathrm{J} = \mathrm{A}$, on aurait $\mathrm{K} \subseteq \mathrm{I}_0$ d'où $b \in \mathrm{I}_0$, contradiction.

D'après le lemme 5.15, (†) entraîne :

$$\sqrt{\mathrm{J}} \bigcap \sqrt{\mathrm{K}} = \sqrt{\mathrm{I}_0} = \mathrm{I}_0.$$

Alors, $\sqrt{\mathrm{J}}$ et $\sqrt{\mathrm{K}}$ sont réduits et propres (car si on avait $1 \in \sqrt{\mathrm{J}}$, on aurait $1 \in \mathrm{J}$ et $\mathrm{J} = \mathrm{A}$, contradiction), et contiennent strictement I_0, donc aucun d'eux n'appartient à $\mathscr{I}$, par maximalité de I_0. Donc, il existe des idéaux premiers $\mathrm{P}_1, \ldots, \mathrm{P}_r$ et $\mathrm{Q}_1, \ldots, \mathrm{Q}_s$ tels que

$$\sqrt{\mathrm{J}} = \bigcap_{i=1}^{r} \mathrm{P}_i, \qquad \sqrt{\mathrm{K}} = \bigcap_{j=1}^{s} \mathrm{Q}_j,$$

d'où

$$\mathrm{I}_0 = \mathrm{P}_1 \bigcap \cdots \bigcap \mathrm{P}_r \bigcap \mathrm{Q}_1 \bigcap \cdots \bigcap \mathrm{Q}_s,$$

contredisant l'hypothèse $\mathrm{I}_0 \in \mathscr{I}$. Cette contradiction montre que $\mathscr{I} = \varnothing$, et donc tout idéal propre réduit I de A est une intersection finie d'idéaux premiers. De plus, si l'on a une écriture

$$\mathrm{I} = \mathrm{P}_1 \bigcap \cdots \bigcap \mathrm{P}_\mathrm{N},$$

et s'il existe $i \neq j$ tels que $\mathrm{P}_i \subseteq \mathrm{P}_j$, on peut supprimer P_j de l'écriture ci-dessus. On se ramène ainsi à une écriture vérifiant la condition $(*)$ du théorème.

Observons que $\mathrm{I} = \mathrm{P}_1 \cap \cdots \cap \mathrm{P}_n$ contient l'idéal produit $\mathrm{P}_1 \cdots \mathrm{P}_n$. Par conséquent, si un idéal premier P contient I, il contient au moins l'un des P_i. Donc si P est minimal, c'est l'un des P_i, et réciproquement chaque P_i est minimal par l'hypothèse $\mathrm{P}_i \not\supseteq \mathrm{P}_j$ si $j \neq i$. Le théorème est démontré. □

Corollaire 11.14. — *Soit* V *une sous-variété algébrique fermée de* $\mathbb{C}^\mathrm{N}$. *Il existe des sous-variétés fermées irréductibles* $\mathrm{V}_1, \ldots, \mathrm{V}_n$ *telles que :*

$$\mathrm{V} = \bigcup_{i=1}^{n} \mathrm{V}_i \qquad \textit{et } \mathrm{V}_i \not\subseteq \mathrm{V}_j \textit{ si } i \neq j.$$

Toute sous-variété irréductible de V *est contenue dans l'une des* V_i, *de sorte que les* V_i *sont exactement les sous-variétés irréductibles maximales de* V. *On les appelle les* **composantes irréductibles** *de* V.

Démonstration. — Elle découle du théorème ci-dessus, et des résultats du paragraphe précédent, et est laissé aux lecteurs intéressés. □

11.4. Topologie de Zariski. — [(2)] Posons $\mathrm{A} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$.

Définition et proposition 11.15 **(Topologie de Zariski)**. —

a) $k^n = \mathscr{V}(\{0\})$ *et* $\varnothing = \mathscr{V}(\{1\}) = \mathscr{V}(k[\mathrm{X}_1, \ldots, \mathrm{X}_n])$.

b) *Soit* $(\mathrm{I}_\lambda)_{\lambda\in\Lambda}$ *une famille quelconque d'idéaux de* A*, alors*

$$\bigcap_{\lambda\in\Lambda} \mathscr{V}(\mathrm{I}_\lambda) = \mathscr{V}(\sum_{\lambda\in\Lambda} \mathrm{I}_\lambda).$$

c) *Soient* I, J *deux idéaux de* A*. On a* $\mathscr{V}(\mathrm{I}) \cup \mathscr{V}(\mathrm{J}) = \mathscr{V}(\mathrm{I} \cap \mathrm{J}) = \mathscr{V}(\mathrm{IJ})$.

Par conséquent, les sous-variétés algébriques fermées de k^n *sont les fermés d'une topologie sur* k^n*, appelée la* **topologie de Zariski**.

Démonstration. — Le point a) est clair. Posons $\Sigma = \sum_{\lambda\in\Lambda} \mathrm{I}_\lambda$. D'après 1), $\mathscr{V}(\Sigma)$ est contenu dans chaque $\mathscr{V}(\mathrm{I}_\lambda)$ et donc dans leur intersection. Réciproquement, soit $x \in \bigcap_\lambda \mathscr{V}(\mathrm{I}_\lambda)$. Alors tout élément de Σ s'annule sur x, d'où $x \in \mathscr{V}(\Sigma)$. Ceci prouve b).

Enfin, comme $\mathrm{IJ} \subseteq \mathrm{I} \cap \mathrm{J} \subseteq \mathrm{I}, \mathrm{J}$, il résulte de 1) que

$$\mathscr{V}(\mathrm{IJ}) \supseteq \mathscr{V}(\mathrm{I} \cap \mathrm{J}) \supseteq \mathscr{V}(\mathrm{I}) \cup \mathscr{V}(\mathrm{J}).$$

Soit $x \in \mathscr{V}(\mathrm{IJ})$ et supposons $x \notin \mathscr{V}(\mathrm{I})$. Il existe donc $\mathrm{P} \in \mathrm{I}$ tel que $\mathrm{P}(x) \neq 0$. Alors, pour tout $\mathrm{Q} \in \mathrm{J}$, l'on a $0 = (\mathrm{PQ})(x) = \mathrm{P}(x)\mathrm{Q}(x)$ et donc $\mathrm{Q}(x) = 0$. Ceci montre que $x \in \mathrm{V}(\mathrm{J})$ et le point c) en découle. La proposition est démontrée. □

Corollaire 11.16. — *Tout sous-ensemble fini* $\mathrm{S} \subset k^n$ *est une sous-variété algébrique fermée de* k^n.

Démonstration. — Tout point x est fermé, car égal à $\mathscr{V}(\mathfrak{m}_x)$. Par conséquent, tout sous-ensemble fini de k^n, étant réunion finie de fermés, est fermé pour la topologie de Zariski. Explicitement, si $\mathrm{X} = \{x_1, \ldots, x_r\}$ alors $\mathrm{X} = \mathscr{V}(\mathfrak{m}_{x_1} \cdots \mathfrak{m}_{x_r})$. □

[(2)] Ce paragraphe n'a pas été traité en cours.

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.

[Ca] J.-C. Carrega, Théorie des corps – La règle et le compas, Hermann, 1981, 2ème édition 1989.

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

[Co] H. S. M. Coxeter, Introduction to Geometry, 2nd edition, Wiley, 1969.

[De] R. Dedekind, Sur la théorie des nombres entiers algébriques, Gauthier-Villars, 1877 ; traduit en anglais avec une introduction de J. Stillwell dans : Theory of algebraic integers, Cambridge Univ. Press, 1996.

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

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

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

[Fu] W. Fulton, Algebraic Curves, Benjamin, 1969.

[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. Nekovář, 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.

[Re] M. Reid, Undergraduate commutative algebra, Cambridge Univ. Press, 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.

[vdW] B. L. van der Waerden, History of algebra from al-Khwarizmi to Emmy Noether, Springer Verlag, 1985.