V. EXTENSIONS ENTIÈRES
(ET ALGÉBRIQUES/TRANSCENDANTES)

Séances des 7 et 13 novembre

14. Extensions entières d'anneaux

14.1. Éléments entiers. — Soit A un anneau commutatif.

***Définition 14.1* (Éléments entiers).** — Soit $\tau : \mathrm{A} \to \mathrm{B}$ une A-algèbre. Par abus de notation, pour $a \in \mathrm{A}$, $b \in \mathrm{B}$, on écrira ab au lieu de $\tau(a)b$. On dit qu'un élément $x \in \mathrm{B}$ est **entier sur** A s'il vérifie une équation de la forme :

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

avec $a_i \in \mathrm{A}$, c.-à-d., si $\mathrm{P}(x) = 0$ pour un certain polynôme **unitaire** $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$. Une telle équation s'appelle une équation de **dépendance intégrale**.

Notation 14.2. — Pour tout $b \in \mathrm{B}$, on note $\mathrm{A}[b]$ la sous-A-algèbre de B engendrée par b. On rappelle que c'est le sous-A-module de B engendré par les monômes b^n, pour $n \in \mathbb{N}$.

***Proposition 14.3* (Caractérisation des éléments entiers).** — *Les conditions suivantes sont équivalentes :*

(i) b *est entier sur* A.

(ii) $\mathrm{A}[b]$ *est un* A*-module de type fini.*

(iii) $\mathrm{A}[b]$ *est contenu dans un sous-anneau* C *de* B *qui est un* A*-module de type fini.*

Démonstration. — Si l'on a une équation de dépendance intégrale $\mathrm{P}(b) = 0$ de degré n, on obtient (par une récurrence sur le degré, ou bien en utilisant la division euclidienne dans $\mathrm{A}[\mathrm{X}]$ par le polynôme unitaire P), que les éléments

(0) Version du 19/11/06

$1, b, \ldots, b^{n-1}$ engendrent $\mathrm{A}[b]$ comme A-module. Ceci montre que (i) $\Rightarrow$ (ii). Il est clair que (ii) $\Rightarrow$ (iii).

Supposons (iii) vérifié et soient $x_1, \ldots, x_n$ des générateurs de C comme A-module. Pour tout i, bx_i appartient à C donc il existe des éléments $a_{ij} \in \mathrm{A}$ tels que

$$(\dagger) \qquad bx_i = \sum_{j=1}^{n} a_{ij} x_j, \qquad \forall\, j = 1, \ldots, n.$$

Désignons par $\mathrm{P} \in \mathrm{M}_n(\mathrm{C})$ la matrice dont le coefficient d'indice (i, j) est $a_{ij} - \delta_{ij} b$, où δ_{ij} désigne le symbole de Kronecker ($\delta_{ij} = 1$ si $i = j$ et $= 0$ sinon). Alors, les équations (†) se récrivent de façon matricielle :

$$(1) \qquad \mathrm{P} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

(Égalité de matrices à coefficients dans l'anneau C). Notons $\widetilde{\mathrm{P}}$ la transposée de la matrice des cofacteurs de P (c.-à-d., $(-1)^{i+j}\widetilde{\mathrm{P}}_{ij}$ égale le déterminant de la matrice obtenue en supprimant dans P la ligne j et la colonne i). Alors, d'après la formule de développement d'un déterminant suivant une ligne ou une colonne, on a l'égalité matricielle :

$$(2) \qquad (\det \mathrm{P})\mathrm{I}_n = \widetilde{\mathrm{P}}\mathrm{P},$$

où I_n désigne la matrice unité. Combiné avec l'égalité (1), ceci donne que l'élément $d := \det \mathrm{P}$ de C vérifie $dx_i = 0$ pour $i = 1, \ldots, n$. Donc d annule le A-module C, et comme C contient l'élément neutre $1 \in \mathrm{B}$, ceci donne $\det \mathrm{P} = 0$. Or, $\mathrm{P} = \mathrm{M} - b\mathrm{I}_n$, où M désigne la matrice dont les coefficients sont les $a_{ij} \in \mathrm{A}$. Donc, en développant $\det \mathrm{P}$, on obtient une égalité

$$(-1)^n b^n + \alpha_1 b^{n-1} + \cdots + \alpha_n = 0,$$

où les α_ℓ sont des polynômes en les a_{ij}, donc appartiennent à A. Ceci montre que b est entier sur A. La proposition est démontrée. □

14.2. Morphismes entiers. —

Définition 14.4. — Soit $\tau : \mathrm{A} \to \mathrm{B}$ une A-algèbre. On dit que B est **entier sur** A si tout élément de B est entier sur A. Dans ce cas, on dit aussi que $\tau : \mathrm{A} \to \mathrm{B}$ est un **morphisme entier**, ou une **extension entière**.

Définition 14.5. — Soit $\tau : \mathrm{A} \to \mathrm{B}$ une A-algèbre.

1) On dit que le morphisme (ou l'extension) $\mathrm{A} \to \mathrm{B}$ est **de type fini** si B est une A-**algèbre** de type fini, c.-à-d., s'il existe $x_1, \ldots, x_n \in \mathrm{B}$ engendrant B comme A-algèbre, c.-à-d., tels que $\mathrm{B} = \mathrm{A}[x_1, \ldots, x_n]$, c.-à-d., si B est

engendrée, comme A-module, par tous les monômes

$$x_1^{\nu_1} \cdots x_n^{\nu_n}, \qquad \text{pour } \nu = (\nu_1, \ldots, \nu_n) \in \mathbb{N}^n.$$

2) On dit que le morphisme (resp. l'extension) $A \to B$ est **fini** (resp. **finie**) si B est un A-**module** de type fini, c.-à-d., s'il existe $m_1, \ldots, m_r \in B$ engendrant B comme A-module, c.-à-d., tels que $B = Am_1 + \cdots + Am_r$.

Remarque 14.6. — 1) Il résulte de la définition que toute extension finie est de type fini, mais la réciproque est fausse. Par exemple, l'extension $k \subset k[X]$ est de type fini, mais n'est pas finie car $k[X]$ n'est pas un k-espace vectoriel de dimension finie (il admet comme base sur k les monômes X^n, pour $n \in \mathbb{N}$).

2) D'après la proposition 14.3, tout morphisme fini est entier.

Remarque 14.7. — Soit $A \to B$ une A-algèbre. Par définition, B est entier sur A si tout $b \in B$ est entier sur A. Évidemment, ceci n'est pas commode à vérifier directement, et donc on a besoin de critères permettant de dire qu'une extension est entière. En particulier, on a le très important point 1) du théorème 14.9 ci-dessous, et le point 2) en conséquence.

Lemme 14.8. — *Soient* $A \subset B$ *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

$$N = Bx_1 + \cdots + Bx_r$$

et chaque Bx_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. □

Théorème 14.9. — 1) **(Critère d'intégralité)** *Soit* $C = A[x_1, \ldots, x_n]$ *une* A*-algèbre de type fini. Si chaque* x_i *est entier sur* A*, alors* C *est un* A*-module de type fini, donc est entier sur* A*.*

2) **(Transitivité des extensions entières)** *Soient* $A \xrightarrow{\tau} B \xrightarrow{\phi} C$*, avec* ϕ *entier. Si* $x \in C$ *est entier sur* B*, alors* x *est entier sur* A*. En particulier, si* C *est entier sur* B*, il est entier sur* A*.*

Démonstration. — 1) Par récurrence sur n. Le cas $n = 1$ a été vu dans la proposition 14.3. On peut donc supposer $n \geqslant 2$ et le résultat établi pour $n-1$. Posons $B = A[x_1, \ldots, x_{n-1}]$. Par hypothèse de récurrence, B est fini sur A. D'autre part, x_n étant entier sur A ; il l'est aussi sur B, et donc $C = B[x_n]$ est fini sur B. Donc, d'après le lemme 14.8, appliqué à $N = C$, on obtient que

C est un A-module de type fini. Donc tout $c \in \mathrm{C}$ est entier sur A, d'après le point (iii) de la proposition 14.3. Ceci prouve le point 1).

2) Par hypothèse, il existe $b_1, \ldots, b_n \in \mathrm{B}$ tels que

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0.$$

Posons $\mathrm{B}_0 := \mathrm{A}[b_1, \ldots, b_n]$. Alors $\mathrm{B}_0[x]$ est fini sur B_0 et, d'après le point 1), B_0 est un A-module de type fini. Donc, d'après le lemme 14.8, le sous-anneau $\mathrm{B}_0[x]$ est un A-module de type fini. D'après la proposition 14.3, ceci entraîne que x est entier sur A. Le théorème est démontré. □

Remarque 14.10. — Dans le point 1), écrivant que chaque x_i vérifie une équation intégrale sur A de degré d_i, on peut aussi montrer par un argument direct que le sous-A-module de C engendré par les monômes

$$x_1^{s_1} \cdots x_n^{s_n}, \quad \text{avec} \quad 0 \leqslant s_i \leqslant d_i$$

est stable par multiplication par chaque x_j, donc coïncide avec C.

14.3. Anneaux intégralement clos. —

Proposition 14.11 **(Clôture intégrale de** A **dans** B**)**. — *Soient* $\mathrm{A} \subset \mathrm{B}$ *des anneaux, et* $\widetilde{\mathrm{A}}$ *l'ensemble des* $b \in \mathrm{B}$ *qui sont entiers sur* A*. Alors* $\widetilde{\mathrm{A}}$ *est un sous-anneau de* B*, appelé la clôture intégrale de* A *dans* B*.*

Démonstration. — D'abord, $\widetilde{\mathrm{A}}$ contient A et donc 1. Soient $x, y \in \widetilde{\mathrm{A}}$. Alors, d'après le point 1) du théorème 14.9, le sous-anneau $\mathrm{A}[x, y]$ est un A-module de type fini. Il contient $x - y$ et xy et donc, d'après le point 3) de la proposition 14.3, $x - y$ et xy sont entiers sur A. Ceci montre que $\widetilde{\mathrm{A}}$ est un sous-anneau de B. □

Définition 14.12. — 1) Soient $\mathrm{A} \subset \mathrm{B}$ deux anneaux. On dit que A est **intégralement fermé dans** B si tout élément de b entier sur A appartient à A, c.-à-d., si A est égal à sa clôture intégrale dans B.

2) On dit qu'un anneau A est **intégralement clos** s'il est **intègre** et s'il est intégralement fermé dans son corps des fractions K, c.-à-d., si tout $\alpha \in \mathrm{K}$ entier sur A appartient à A.

Corollaire 14.13. — *Soient* $\mathrm{A} \subset \mathrm{B}$ *deux anneaux et* $\widetilde{\mathrm{A}}$ *la clôture intégrale de* A *dans* B*. Alors* $\widetilde{\mathrm{A}}$ *est intégralement fermé dans* B*. En particulier, si* A *est intègre et si* $\widetilde{\mathrm{A}}$ *est la clôture intégrale de* A *dans son corps des fractions, alors* $\widetilde{\mathrm{A}}$ *est intégralement clos.*

Démonstration. — Soit $x \in \mathrm{B}$ entier sur $\widetilde{\mathrm{A}}$. D'après le point 2) du théorème 14.9, x est entier sur A, donc appartient à $\widetilde{\mathrm{A}}$. □

Les anneaux intégralement clos jouent un rôle important en géométrie algébrique et en théorie des nombres ; voir par exemple [**AM**, Chap.9], [**Die**, § 5], [**Sa**]. On a d'autre part l'important résultat suivant.

Proposition 14.14. — *Soit* A *factoriel. Alors* A *est intégralement clos.*

Démonstration. — Soient K le corps des fractions de A et $\alpha \in \mathrm{K} \setminus \{0\}$. On peut écrire $\alpha = b/c$, avec b et c sans facteur commun. Supposons α entier sur A. Alors il existe $a_1, \ldots, a_n \in \mathrm{A}$ tels que

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0.$$

Multipliant cette égalité par c^n, on obtient que

$$(*) \qquad -b^n = ca_1b^{n-1} + \cdots + c^n a_n$$

est divisible par c. Ceci entraîne que c est inversible dans A. En effet, sinon soit p un élément irréductible divisant c. D'après $(*)$ il divise b^n et donc, d'après le Lemme d'Euclide (puisque A est factoriel), p divise b, une contradiction. Donc c est un élément inversible de A et $\alpha \in \mathrm{A}$. La proposition est démontrée. □

Corollaire 14.15. — *Si* $q \in \mathbb{Q}$ *est entier sur* $\mathbb{Z}$ *alors* $q \in \mathbb{Z}$.

Ceci explique la terminologie d'« éléments entiers ».

14.4. Extensions entières et idéaux premiers. —

Proposition 14.16. — *Soit* $\mathrm{A} \subset \mathrm{B}$ *une extension entière.*

1) *Soient* J *un idéal propre de* B *et* $\mathrm{I} = \mathrm{A} \cap \mathrm{J}$. *Alors l'extension* $\mathrm{A/I} \subseteq \mathrm{B/J}$ *est entière.*

2) *Si* S *est une partie multiplicative de* A, *l'extension* $\mathrm{S^{-1}A} \subseteq \mathrm{S^{-1}B}$ *est entière.*

Démonstration. — Facile, et laissée au lecteur. □

Proposition 14.17. — *Soient* $\mathrm{A} \subseteq \mathrm{B}$ *deux anneaux commutatifs* **intègres**, *avec* B **entier** *sur* A. *Alors :*

$$\mathrm{A} \text{ est un corps} \Leftrightarrow \mathrm{B} \text{ est un corps.}$$

Démonstration. — Supposons que A soit un corps. Soit b un élément non nul de B. Considérons une équation de dépendance intégrale de degré minimal :

$$b^n + a_1b^{n-1} + \cdots + a_n = 0,$$

avec $a_i \in \mathrm{A}$. Alors $a_n \neq 0$, car sinon, comme B est intègre, on aurait $b^{n-1} + \cdots + a_{n-1} = 0$, contredisant la minimalité de n. Donc, comme A est un corps, a_n est inversible, d'où

$$-b(b^{n-1} + \cdots + a_{n-1})a_n^{-1} = 1.$$

Ceci montre que b est inversible, et donc B est un corps.

Réciproquement, supposons que B soit un corps et soit $a \in \mathrm{A}$, non nul. Alors, a admet dans B un inverse b, et b est entier sur A. Donc il existe $n \in \mathbb{N}^*$ et $c_1, \ldots, c_n \in \mathrm{A}$ tels que

$$b^n = c_1 b^{n-1} + \cdots + c_n.$$

Multipliant cette égalité par a^{n-1}, on obtient que $b \in \mathrm{A}$. Ceci prouve la proposition. □

Corollaire 14.18. — *Soit* $\phi : \mathrm{A} \to \mathrm{B}$ *un morphisme entier et soient* $\mathfrak{q} \in \mathrm{Spec(B)}$ *et* $\mathfrak{p} = \phi^{-1}(\mathfrak{q})$. *Alors* $\mathfrak{q}$ *est maximal si et seulement si* $\mathfrak{p}$ *l'est.*

Démonstration. — Remplaçant B par $\mathrm{B}/\mathfrak{q}$ et A par $\mathrm{A}/\mathfrak{p}$, on obtient un morphisme injectif et entier $\mathrm{A} \hookrightarrow \mathrm{B}$, et le résultat découle de la proposition précédente. □

Signalons aussi le lemme ci-dessous, qu'il est utile de connaître, et qui fournit une autre démonstration de l'implication $\Rightarrow$ dans la proposition 14.17.

Lemme 14.19. — *Soient* k *un corps et* B *une* k*-algèbre intègre de dimension finie. Alors* B *est un corps.*

Démonstration. — Soit $b \neq 0$ dans B. L'application $\rho_b : \mathrm{B} \to \mathrm{B}$, $x \mapsto bx$ est k-linéaire, et elle est injective car B est intègre. Puisque B est un k-espace vectoriel de dimension finie, ρ_b est donc bijective. Il existe donc $x \in \mathrm{B}$ tel que $bx = 1$, ce qui montre que b est inversible. □

15. Extensions de corps

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

Remarque 15.1. — Soient K et K′ deux corps et soit $\phi : \mathrm{K} \to \mathrm{K}'$ un morphisme d'anneaux. Alors :

a) ϕ est **injectif** car $\operatorname{Ker}\phi$, étant un idéal propre de K (car $\phi(1) = 1$), 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 15.2. — 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.

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 15.3. — *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. — C'est clair. □

Définition 15.4 **(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 15.5 **(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 15.6. — *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 15.7. — Dans ce cours, on ne considèrera que des extensions de type fini. Mais les extensions de type infini existent dans la nature. Par exemple, l'extension $\mathbb{Q} \subseteq \mathbb{R}$ n'est pas de type fini, car on peut montrer que $\mathbb{R}$ est de degré de transcendance (voir 15.35 plus bas) infini sur $\mathbb{Q}$.

Définition 15.8. — 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 $\phi \circ \tau = \tau'$.

15.2. Sous-corps premier et caractéristique. — Il y a deux exemples fondamentaux de corps. D'une part, le corps des rationnels $\mathbb{Q}$, qui est le corps des fractions de $\mathbb{Z}$. D'autre part, les corps finis $\mathbb{F}_p = \mathbb{Z}/\mathbb{Z}_p$, où $p \in \mathbb{Z}$ est un nombre premier.

Définition 15.9. — Soit $p \geqslant 2$ un nombre premier. On note $\mathbb{F}_p$ l'anneau quotient $\mathbb{Z}/p\mathbb{Z}$. C'est un corps car l'idéal $p\mathbb{Z}$ est maximal, puisque $\mathbb{Z}$ est principal et p irréductible.

De façon équivalente, mais plus concrète, le fait que $\mathbb{Z}/(p)$ soit un corps résulte du théorème de Bezout. En effet, soit $a \in \mathbb{Z}$ non divisible par p. Comme l'idéal engendré par a et p est $\mathbb{Z}$, il existe $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha a + \beta p = 1$. Alors, les classes de α et a modulo p sont inverses l'une de l'autre.

En pratique, on peut trouver explicitement les « coefficients de Bezout » α et β (et donc l'inverse α de a modulo p), par la méthode des divisions successives.

Exemples 15.10. — **1)** Prenons $p = 37$ et $a = 7$. Alors

$$\begin{cases} 37 = 5 \times 7 + 2 \\ 3 \times 2 + 1 = 7, \end{cases} \quad \text{d'où} \quad \begin{cases} 3 \cdot 37 = 15 \times 7 + 3 \times 2 \\ 3 \times 2 + 1 = 7, \end{cases}$$

et $16 \cdot 7 - 3 \cdot 37 = 1$. Donc l'inverse de 7 mod. 37 est 16.

2) Prenons $p = 167$ et $a = 17$. Alors

$$\begin{cases} 167 = 9 \times 17 + 14 \\ 14 + 3 = 17 \\ 14 = 4 \times 3 + 2 \\ 1 + 2 = 3, \end{cases} \quad \text{d'où} \quad \begin{cases} 14 + 1 = 5 \times 3, \\ 6 \times 14 + 1 = 5 \times 17, \\ 6 \times 167 + 1 = (6 \cdot 9 + 5) \times 17. \end{cases}$$

Donc $1 = 59 \cdot 17 - 6 \cdot 167$ et 59 est l'inverse de 17 modulo 167.

Lemme 15.11. — *Soit* A *un anneau. Il existe un unique morphisme d'anneaux* $\phi : \mathbb{Z} \to \mathrm{A}$.

Démonstration. — Comme A est un groupe abélien, c'est un $\mathbb{Z}$-module, pour l'action définie, pour tout $n \geqslant 0$ et $x \in \mathrm{A}$, par $n \cdot x = x + \cdots + x$ (n fois), et $(-n)\cdot x = n\cdot(-x)$. De plus, le morphisme de $\mathbb{Z}$-modules $\phi : \mathbb{Z} \to \mathrm{A}$, $n \mapsto n\cdot 1$ est un morphisme d'anneaux, puisque la distributivité de la multiplication dans A entraîne :

$$(m \cdot 1)(n \cdot 1) = (1 + \cdots + 1)(1 + \cdots + 1) = (mn) \cdot 1.$$

Ceci prouve l'existence. Réciproquement, si $\psi : \mathbb{Z} \to \mathrm{A}$ est un morphisme d'anneaux, alors $\psi(1) = 1$ et $\psi(n) = n \cdot 1$ pour tout $n \in \mathbb{Z}$, donc $\psi = \phi$. □

Rappelons la définition suivante, déjà introduite en 15.4

Définition 15.12. — 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.

***Théorème 15.13* (Caractéristique et sous-corps premier)**

Soit K *un corps. Son sous-corps premier est isomorphe soit à* $\mathbb{Q}$*, soit à* $\mathbb{F}_p$*, pour un nombre premier* $p \geqslant 2$ *uniquement déterminé. On dit que la* **caractéristique** *de* K *est* 0 *dans le premier cas, et* p *dans le second cas.*

De façon plus précise, la caractéristique de K *est le générateur* $\geqslant 0$ *du noyau du morphisme* $\mathbb{Z} \to \mathrm{K}$*,* $n \mapsto n \cdot 1_{\mathrm{K}}$*. On la note* $\mathrm{car}(\mathrm{K})$*.*

Démonstration. — Soit ϕ l'unique morphisme d'anneaux $\mathbb{Z} \to \mathrm{K}$. Alors $\operatorname{Ker}\phi$ est un idéal premier de $\mathbb{Z}$, puisque $\mathbb{Z}/\operatorname{Ker}\phi$ est isomorphe à un sous-anneau de K, donc intègre. Par conséquent, de deux choses l'une.

1) Si $\operatorname{Ker}\phi = (0)$, on peut identifier $\mathbb{Z}$ à son image $\mathbb{Z}1_{\mathrm{K}}$. Comme tout élément de $\phi(\mathbb{Z} \setminus \{0\})$ est inversible dans K, alors ϕ se prolonge en un morphisme d'anneaux $\psi : \mathbb{Q} \to \mathrm{K}$, nécessairement injectif puisque $\mathbb{Q}$ est un corps. De plus, tout sous-corps de K contient 1_{K}, les éléments $n \cdot 1_{\mathrm{K}}$ et leurs inverses. Ceci montre que le sous-corps premier de K est $\psi(\mathbb{Q})$, isomorphe à $\mathbb{Q}$. Dans ce cas, on identifiera $\mathbb{Q}$ à son image dans K :

$$\mathbb{Q} = \{x \in \mathrm{K} \mid \exists\, n, m \in \mathbb{Z}, n \neq 0, \text{ tels que } nx = m1_{\mathrm{K}}\}.$$

2) Si $\operatorname{Ker}\phi \neq (0)$, alors $\operatorname{Ker}\phi = (p)$, où p est un nombre premier $\geqslant 2$ uniquement déterminé. Dans ce cas, ϕ induit un isomorphisme de $\mathbb{F}_p$ sur son image, qui est formée des éléments $n1_{\mathrm{K}}$ pour $0 \leqslant n < p$. Ceci montre que, dans ce cas, le sous-corps premier de K est formé des éléments $n1_{\mathrm{K}}$ pour $0 \leqslant n < p$; on l'identifiera à $\mathbb{F}_p$. Le théorème est démontré. □

15.3. L'alternative algébrique/transcendant. — Soit $k \subset \mathrm{K}$ une extension de corps et soit $\alpha \in \mathrm{K}$. On note $k[\alpha]$ la **sous-k-algèbre** de K engendrée par α.

Soit $\phi_\alpha : k[\mathrm{X}] \to \mathrm{K}$ le morphisme de k-algèbres défini par $\phi_\alpha(\mathrm{X}) = \alpha$. Alors $\phi_\alpha(\mathrm{P}) = \mathrm{P}(\alpha) \in \mathrm{K}$, pour tout $\mathrm{P} \in k[\mathrm{X}]$, et l'image de ϕ_α est $k[\alpha]$. Posons

$\mathrm{I}_\alpha = \operatorname{Ker}\phi_\alpha$. Puisque $k[\mathrm{X}]/\mathrm{I}_\alpha \cong k[\alpha]$ est intègre, alors I_α est un idéal premier de $k[\mathrm{X}]$. Donc, de deux choses l'une : ou bien $\mathrm{I}_\alpha = (0)$ ou bien $\mathrm{I}_\alpha = (\mathrm{P})$ pour un polynôme irréductible unitaire uniquement déterminé.

Définition 15.14 **(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 ; par conséquent, α est **entier** sur k.

Le polynôme P est appelé **polynôme minimal de α sur k** ; on le notera $\operatorname{Irr}_k(\alpha)$. Son degré s'appelle **degré de α sur k** et se note $\deg_k(\alpha)$.

Remarque 15.15. — 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 $\operatorname{Irr}_k(\alpha)$ est divisible, dans $\mathrm{L}[\mathrm{X}]$, par $\operatorname{Irr}_{\mathrm{L}}(\alpha)$.

Théorème 15.16 **(Extensions monogènes $k(x)$)**. — *Supposons* $\mathrm{K} = k(x)$.

1) *Si x est algébrique sur k, alors* $\operatorname{Irr}_k(x)$ *est irréductible et l'on a*

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

Par conséquent, les éléments $1, x, \dots, x^{d-1}$*, 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, $\mathrm{I}_x = (\operatorname{Irr}_k(x))$ est premier. D'après le lemme 15.26, $\operatorname{Irr}_k(x)$ est irréductible et engendre un idéal maximal de $k[\mathrm{X}]$. Donc, $\mathrm{A} := k[\mathrm{X}]/(\operatorname{Irr}_k(x))$ 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 $1, \dots, \mathrm{X}^{d-1}$ 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 $\phi(k[\mathrm{X}] \setminus \{0\})$ est inversible dans K, et donc ϕ se prolonge 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 $k(\mathrm{X}) \xrightarrow{\sim} k(x) = \mathrm{K}$. □

Remarque 15.17. — Écrivons $\operatorname{Irr}_k(x) = x^d + a_1 x^{d-1} + \cdots + a_d$ et observons que $a_d \neq 0$ puisque $\operatorname{Irr}_k(x)$ est irréductible. Alors l'inverse de x est égal à

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

D'autre part, le fait que, dans ce cas, $k[x]$ coïncide avec $k(x)$ résulte aussi du lemme 14.19.

15.4. Extensions algébriques et degré. — On a vu plus haut 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 15.18. — Soit K/k une extension ; $\dim_k \mathrm{K}$ s'appelle **degré de** K **sur** k et se note $[\mathrm{K} : k]$. C'est un élément de $\mathbb{N}^* \cup \{+\infty\}$.

Proposition 15.19 **(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 :

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

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

2) De façon plus concrète, 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, cf. la preuve du lemme 14.8. 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 15.20. — 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.

Définition 15.21. — 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.

Remarque 15.22. — Soit k un corps. La notion d'élément algébrique sur k coïncide avec celle d'élement entier, et donc une extension de corps K/k est algébrique si et seulement si c'est une extension entière. On peut donc déduire des résultats sur les extensions entières les résultats suivants.

Théorème 15.23. — *Soit* K/k *une extension de corps.*

1) **(Critère d'algébricité)** *Si* $\mathrm{K} = k(x_1, \ldots, x_n)$ *et si chaque* x_i *est* **algébrique** *sur* k *de degré* d_i*, alors* $\mathrm{K} = k[x_1, \ldots, x_n]$*, c.-à-d.,* K *est engendré comme* k**-algèbre** *par les* x_i*, et* K/k *est* **algébrique** *et* **de degré fini** *; plus précisément, on a*

$$[\mathrm{K} : k] \leqslant d_1 \cdots d_n.$$

2) **(Transitivité des extensions algébriques)** *Si les extensions* K/k *et* L/K *sont algébriques, alors* L/k *l'est aussi.*

Démonstration. — 1) Montrons que $\mathrm{K} = k[x_1, \ldots, x_n]$ et $[\mathrm{K} : k] \leqslant d_1 \cdots d_n$ par récurrence sur n. Si $n = 1$, c'est le théorème 15.16. On peut donc supposer $n \geqslant 2$ et l'assertion établie pour $n - 1$. Posons $\mathrm{K}' = k(x_1, \ldots, x_{n-1})$. Alors $\mathrm{K} = \mathrm{K}'(x_n)$ et x_n est algébrique sur K' de degré $\leqslant d_n$ et donc, par l'hypothèse de récurrence plus le cas $n = 1$ appliqué à K', on obtient :

$$(*) \qquad \mathrm{K} = \mathrm{K}'(x_n) = \mathrm{K}'[x_n] = k[x_1, \ldots x_n],$$

et

$$[\mathrm{K} : k] = [\mathrm{K} : \mathrm{K}']\,[\mathrm{K}' : k] \leqslant d_n d_{n-1} \cdots d_1.$$

Ceci achève la récurrence. Donc K est de degré fini sur k, et donc tout élément de K est algébrique sur k, d'après la proposition 14.3 ou bien le point 2) du théorème 15.16. Le point 1) est démontré.

Le point 2) découle du point 2) du théorème 14.9. □

Remarque 15.24. — Une autre démonstration du point 1) du théorème 15.23 est la suivante. Soit $\phi : k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \to \mathrm{K}$ le morphisme de k-algèbres défini par $\phi(\mathrm{X}_i) = x_i$, pour $i = 1, \ldots, n$; on a $\phi(\mathrm{P}) = \mathrm{P}(x_1, \ldots, x_n) \in \mathrm{K}$ pour tout $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. L'image de ϕ est $\mathrm{A} := k[x_1, \ldots, x_n]$, la sous-$k$-algèbre de K engendré par les x_i. Comme chaque monôme x_i^n est combinaison k-linéaire des monômes x_i^r, avec $0 \leqslant r < d_i$, on en déduit que A est engendrée sur k par les monômes

$$x_1^{r_1} \cdots x_n^{r_n},$$

où $r_i < d_i$ pour tout i. Par conséquent, A est une k-algèbre de dimension finie $\leqslant d_1 \cdots d_n$. De plus, A est intègre, puisque contenue dans K. D'après le lemme 14.19, A est un corps, et l'égalité $(*)$ en résulte. Donc $\mathrm{K} = \mathrm{A}$ est de dimension $\leqslant d_1 \cdots d_n$ sur k.

Corollaire 15.25. — *Une extension de corps $k \subset \mathrm{K}$ est de degré fini si et seulement si elle est algébrique et de type fini.*

15.5. Un théorème de Zariski. — [(1)] Commençons par rappeler le lemme suivant, déjà vu précédemment.

Lemme 15.26. — *Soient* K *un corps et* $\mathfrak{p}$ *un idéal premier non nul de* $\mathrm{K}[\mathrm{X}]$. *Alors* $\mathfrak{p} = (\mathrm{P})$, *où* P *est un polynôme irréductible,* $\mathfrak{p}$ *est maximal et* $\mathrm{K}[\mathrm{X}]/\mathfrak{p}$ *est de degré* $\deg \mathrm{P}$ *sur* K.

Démonstration. — Comme $\mathrm{K}[\mathrm{X}]$ est principal (11.36), $\mathfrak{p} = (\mathrm{P})$ pour un certain polynôme unitaire de degré $d \geqslant 1$. Si on avait $\mathrm{P} = \mathrm{QR}$ avec $\deg \mathrm{Q}, \deg \mathrm{R} < \deg \mathrm{P}$, on aurait $\mathrm{Q}, \mathrm{R} \notin \mathfrak{p}$ mais $\mathrm{QR} = \mathrm{P} \in \mathfrak{p}$, contredisant le fait que $\mathfrak{p}$ est premier. Ceci montre que P est irréductible.

Par conséquent, si $\mathrm{Q} \in \mathrm{K}[\mathrm{X}] \setminus \mathfrak{p}$ il existe $\mathrm{A}, \mathrm{B} \in \mathrm{K}[\mathrm{X}]$ tels que $\mathrm{AP} + \mathrm{BQ} = 1$. Ceci montre que $\mathfrak{p} = (\mathrm{P})$ est un idéal maximal.

Enfin, soit x l'image de X dans $\mathrm{L} := \mathrm{K}[\mathrm{X}]/(\mathrm{P})$. D'une part, en utilisant la division euclidienne, on voit que les éléments $1, x, \ldots, x^{d-1}$ (où $d = \deg \mathrm{P}$) engendrent L comme K-espace vectoriel. D'autre part, ces éléments sont linéairement indépendants sur K, car si $a_0 + a_1 x + \cdots + a_{d-1} x^{d-1} = 0$, alors le polynôme $a_0 + \cdots + a_{d-1} \mathrm{X}^{d-1}$ est divisible par P (de degré d), ce qui n'est possible que si $a_i = 0$ pour $i = 0, \ldots, d-1$. Donc $\{1, x, \ldots, x^{d-1}\}$ est une base de L sur K, et $[\mathrm{L} : \mathrm{K}] = d = \deg \mathrm{P}$. Le lemme est démontré. □

***Théorème 15.27* (Zariski)**. — *Soient* K *un corps et* $\mathfrak{m}$ *un idéal maximal de* $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. *Alors le corps* $\mathrm{L} = \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathfrak{m}$ *est une extension de degré fini de* K.

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

Démonstration. — On procède par récurrence sur n. Si $n = 1$, alors $\mathfrak{m} = (\mathrm{P})$, pour un certain polynôme irréductible de degré $d \geqslant 1$, et $\mathrm{K}[\mathrm{X}]/(\mathrm{P})$ est de degré d sur K, d'après le lemme 15.26.

Supposons $n > 1$ et le théorème démontré pour $n - 1$, pour tout corps. Notons x_i l'image de X_i dans L et observons que les x_i engendrent L comme K-algèbre, c.-à-d., on a

$$\mathrm{L} = \mathrm{K}[x_1, \ldots, x_n]. \tag{\dagger}$$

Soit $\mathrm{I} := \mathfrak{m} \cap \mathrm{K}[\mathrm{X}_1]$; c'est un idéal premier de $\mathrm{K}[\mathrm{X}_1]$. Montrons d'abord que $\mathrm{I} \neq (0)$.

Supposons le contraire. Alors le morphisme $\mathrm{K}[\mathrm{X}_1] \to \mathrm{L}$ est injectif, donc se prolonge en un morphisme de corps $\mathrm{K}(\mathrm{X}_1) \hookrightarrow \mathrm{L}$. D'après (†), L est *a fortiori* engendré comme $\mathrm{K}(\mathrm{X}_1)$-algèbre par $x_2, \ldots, x_n$, donc égale $\mathrm{K}(\mathrm{X}_1)[\mathrm{X}_2, \ldots, \mathrm{X}_n]/\mathfrak{m}'$, pour un certain idéal maximal $\mathfrak{m}'$.

Par hypothèse de récurrence, L est de dimension finie sur $\mathrm{K}(\mathrm{X}_1)$. Donc, chaque x_i est racine d'un polynôme unitaire $\mathrm{P}_i(\mathrm{T}) \in k(\mathrm{X}_1)[\mathrm{T}]$. Soit $f \in \mathrm{K}[\mathrm{X}_1]$ un dénominateur commun aux coefficients de $\mathrm{P}_2, \ldots, \mathrm{P}_n$. Alors chaque x_i est entier sur le sous-anneau $\mathrm{K}[\mathrm{X}_1][1/f]$ de L. Comme

$$\mathrm{L} = (\mathrm{K}[\mathrm{X}_1][1/f])[x_2, \ldots, x_n],$$

il résulte du théorème 14.9, que L est entier sur $\mathrm{K}[\mathrm{X}_1][1/f]$. Donc, d'après la proposition 14.17, $\mathrm{K}[\mathrm{X}_1][1/f]$ est un corps. Mais ceci n'est pas possible. En effet, si on avait $\deg f = 0$, c.-à-d., $f \in \mathrm{K}$, ceci dirait que $\mathrm{K}[\mathrm{X}_1]$ est un corps, ce qui n'est pas le cas. Donc $\deg f > 0$. Mais alors $1 + f$ est non nul et n'est pas inversible dans $\mathrm{K}[\mathrm{X}_1][1/f]$. En effet, on aurait sinon $(1 + f)\mathrm{P} = f^r$, avec $\mathrm{P} \in \mathrm{K}[\mathrm{X}_1]$ et $r \geqslant 1$, et comme $\mathrm{K}[\mathrm{X}]$ est factoriel (Thm. 11.36) et $1 + f$ et f^r sont premiers entre eux, f^r diviserait P, et donc $1 + f$ serait inversible dans $\mathrm{K}[\mathrm{X}_1]$, absurde puisque $\deg f > 0$.

Cette contradiction montre que I est un idéal premier non nul de $\mathrm{K}[\mathrm{X}_1]$. Donc, d'après le lemme 15.26, c'est un idéal maximal et $\mathrm{K}' := \mathrm{K}[\mathrm{X}_1]/\mathrm{I}$ est un corps de degré fini sur K. De plus, L est un quotient de $\mathrm{K}'[\mathrm{X}_2, \ldots, \mathrm{X}_n]$ donc, par hypothèse de récurrence, L est de degré fini sur K′, et donc aussi sur K (d'après 15.19). Ceci prouve le théorème. □

***Définition 15.28* (Les idéaux $\mathfrak{m}_x$, pour $x \in k^n$).** — Pour tout $x \in k^n$, notons $\mathfrak{m}_x$ l'idéal engendré par $\mathrm{X}_1 - x_1, \ldots, \mathrm{X}_n - x_n$. C'est le noyau du morphisme surjectif de k-algèbres

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

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 un idéal I arbitraire, on a :

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

On pose alors

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

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 15.29* (Théorème des zéros, forme faible).** — *On suppose k algébriquement clos.*

1) *Soit $\mathfrak{m}$ un idéal maximal de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Alors $\mathfrak{m} = \mathfrak{m}_x$, pour un unique $x \in k^n$.*

2) *Soit* J *un idéal propre de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Alors $\mathscr{V}(\mathrm{J}) \neq \varnothing$.*

Démonstration. — 1) Comme k est algébriquement clos, le théorème précédent 15.27 entraîne que $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathfrak{m} = k$. Notant x_i l'image de X_i dans k et posant $x = (x_1, \ldots, x_n)$, 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. Il est contenu dans un idéal maximal $\mathfrak{m}_x$, et donc $\mathscr{V}(\mathrm{J})$ contient x. Le théorème est démontré. □

15.6. Bases de transcendance. — [(2)] Afin de couvrir les extensions de type fini K/k arbitraires (c.-à-d., pas nécessairement algébriques), traitons dans ce paragraphe la notion de base (et degré) de transcendance

Soit K/k une extension de corps, et soient $x_1, \ldots, x_n \in \mathrm{K}$.

Définition 15.30. — On dit que $x_1, \ldots, x_n$ sont **algébriquement indépendants sur** k si le morphisme

$$\phi : k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \longrightarrow \mathrm{K}, \qquad \mathrm{P} \mapsto \mathrm{P}(x_1, \ldots, x_n)$$

est injectif. Dans ce cas, ϕ se prolonge en un isomorphisme de $k(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ sur le sous-corps de K engendré par les x_i. En particulier, chaque x_i est transcendant sur k.

Remarque 15.31. — Soit K le corps des fractions de l'anneau $k[x, y]$, où $x^2 = y^3$. Alors x et y sont transcendants sur k, mais ne sont pas algébriquement indépendants sur k, puisqu'on a la relation $x^2 = y^3$.

Définition 15.32. — On dit qu'une partie B de K est une **base de transcendance sur** k si elle vérifie les deux conditions suivantes :

(i) les éléments de B sont algébriquement indépendants sur k ;

(ii) le corps K est extension algébrique du sous-corps $k(\mathrm{B})$.

Ceci équivaut à dire que B est une partie **algébriquement indépendante maximale**.

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

Lemme 15.33. — *Soit* K/k *une extension et soit* S *une partie* **finie** *de* K *telle que* K *soit algébrique sur* $k(\mathrm{S})$. *Alors* S *contient une base de transcendance* B *de* K *sur* k. *De plus,* $[k(\mathrm{S}) : k(\mathrm{B})] < \infty$ *; en particulier, si* $\mathrm{K} = k(\mathrm{S})$, *alors* K *est de degré fini sur* $k(\mathrm{B})$.

Démonstration. — Posons $\mathrm{S} = \{x_1, \ldots, x_n\}$. Quitte à renuméroter les x_i, on peut supposer que $x_1, \ldots, x_r$ sont algébriquement indépendants sur k et que, pour tout $i > r$, x_i est algébrique sur $k(\mathrm{B})$, où $\mathrm{B} = \{x_1, \ldots, x_r\}$. Alors, par transitivité des extensions algébriques (15.23), K est algébrique sur $k(\mathrm{B})$, et donc B est une base de transcendance de K sur k.

De plus, d'après le théorème 15.23, $k(\mathrm{S})$ est de degré fini sur $k(\mathrm{B})$. □

Proposition 15.34. — *Soit* K/k *une extension de corps telle que* K *possède une base de transcendance sur* k **finie**.

1) *Soit* B *une base de transcendance de* K *sur* k *de cardinal* **minimum** n. *Alors, toute partie* B' *algébriquement indépendante sur* k *est de cardinal* $\leqslant n$.

2) *Par conséquent,* **toute** *base de transcendance de* K *sur* k *est de cardinal* n.

Démonstration. — On procède par récurrence sur l'entier $s(\mathrm{B}, \mathrm{B}') := \#\mathrm{B} - \#(\mathrm{B} \cap \mathrm{B}')$. Si $s = 0$, alors $\mathrm{B} \subseteq \mathrm{B}'$ donc $\mathrm{B}' = \mathrm{B}$ par maximalité de B. On peut donc supposer $s \geqslant 1$ et l'assertion établie pour $s - 1$.

Écrivons $\mathrm{B} = \{b_1, \ldots, b_n\}$. Sans perte de généralité, on peut supposer que

$$\mathrm{B} \cap \mathrm{B}' = \{b_{s+1}, \ldots, b_n\}.$$

Si $\mathrm{B}' \subseteq \mathrm{B}$, l'assertion est vérifiée, donc on peut supposer qu'il existe $b' \in \mathrm{B}'$ tel que $b' \notin \mathrm{B}$. Alors $\mathrm{B} \cup \{b'\}$ n'est pas algébriquement indépendante, par maximalité de B. Donc, il existe $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n, \mathrm{X}_{n+1}]$ non nul tel que

$$\mathrm{P}(b_1, \ldots, b_n, b') = 0.$$

De plus, $\mathrm{P} \notin k[\mathrm{X}_{s+1}, \ldots, \mathrm{X}_{n+1}]$, puisque les éléments de B' sont algébriquement indépendants. Donc, sans perte de généralité, on peut supposer que P contient la variable X_1.

Posons alors $\mathrm{B}_1 = \{b_2, \ldots, b_n, b'\}$. Alors b_1 est algébrique sur $k(\mathrm{B}_1)$, et comme K est algébrique sur $k(\mathrm{B}_1)[b_1]$, il est aussi algébrique sur $k(\mathrm{B}_1)$.

Comme $\#\mathrm{B}_1 = n$, la minimalité de n, jointe au lemme 15.33, entraîne que B_1 est une base de transcendance de K sur k (car sinon, B_1 contiendrait une base de transcendance de K sur k de cardinal $< n$, contredisant la minimalité de n). De plus,

$$\#\mathrm{B}_1 - \#(\mathrm{B}_1 \cap \mathrm{B}') = s - 1, \quad \text{car} \quad \mathrm{B}_1 \cap \mathrm{B}' = \{b_{s+1}, \ldots, b_n, b'\}.$$

Donc, par l'hypothèse de récurrence, appliquée à B_1 et B', on obtient que $\#\mathrm{B}' \leqslant \#\mathrm{B}_1 = n$. Ceci prouve 1).

En particulier, si B' est une autre base de transcendance de K/k, alors $\#\mathrm{B}' \leqslant n$, et donc $\#\mathrm{B}' = n$ par minimalité de n. La proposition est démontrée. □

Théorème 15.35. — *Soit $k \subset \mathrm{K}$ une extension de corps de type fini. Alors :*

1) *Toutes les bases de transcendance de* K *ont le même cardinal, appelé* **degré de transcendance de** K **sur** k *et noté* $\deg \mathrm{tr}_k \mathrm{K}$. *De plus, tout ensemble d'éléments algébriquement indépendants est contenu dans une base de transcendance.*

2) *Soit* L/k *une sous-extension de* K/k (*c.-à-d.,* L *est un sous-corps de* K *contenant* k). *Alors* L/k *est de type fini et l'on a*

$$\deg \mathrm{tr}_k \mathrm{L} \leqslant \deg \mathrm{tr}_k \mathrm{K}.$$

Démonstration. — D'après le lemme 15.33, il existe une base de transcendance B_0 de K sur k ayant r éléments. Alors, d'après la proposition précédente, toute base de transcendance de K sur k a r éléments, et toute partie algébriquement libre est de cardinal $\leqslant r$. Par conséquent, toute suite croissante de parties algébriquement indépendantes est stationnaire (après au plus r étapes), et donc toute partie algébriquement indépendante est contenue dans une partie algébriquement indépendante maximale, c.-à-d., dans une base de transcendance de K sur k. Ceci prouve 1).

Démontrons 2). Comme toute partie de L algébriquement indépendante sur k est aussi une partie de K algébriquement indépendante sur k, on obtient que L possède une base de transcendance finie $\mathrm{B} = \{b_1, \ldots, b_t\}$, qu'on peut compléter en une base de transcendance

$$\widetilde{\mathrm{B}} = \mathrm{B} \sqcup \mathrm{C} = \{b_1, \ldots, b_t\} \sqcup \{c_1, \ldots, c_s\}$$

de K sur k (où $t + s = r = \deg \mathrm{tr}_k \mathrm{K}$). Montrons que L est de degré fini sur $k(\mathrm{B})$. Ceci va résulter du lemme suivant.

Lemme 15.36. — C *est algébriquement indépendante sur* L.

Démonstration. — Sinon, il existe un polynôme $\mathrm{P} \in \mathrm{L}[\mathrm{X}_1, \ldots, \mathrm{X}_s]$ non nul tel que $\mathrm{P}(c_1, \ldots, c_s) = 0$. Sans perte de généralité, on peut supposer que X_s apparaît dans P, et donc que c_s est algébrique sur $\mathrm{L}(\mathrm{C}')$, où $\mathrm{C}' = \{c_1, \ldots, c_{s-1}\}$. Or,

$$\mathrm{L}(c_1, \ldots, c_{s-1}) = k(\mathrm{B} \cup \mathrm{C}')(\mathrm{L})$$

est algébrique sur $k(\mathrm{B} \cup \mathrm{C}')$, puisque L est algébrique sur $k(\mathrm{B})$. Donc, d'après la transitivité des extensions entières (14.9), c_s est algébrique sur $k(\mathrm{B} \cup \mathrm{C}')$, une contradiction. Ceci prouve le lemme. □

On peut maintenant achever la preuve du théorème. Soient $\ell_1, \dots, \ell_n$ des éléments de L linéairement indépendants sur $k(\mathrm{B})$. Montrons qu'ils sont encore linéairement indépendants sur $k(\widetilde{\mathrm{B}})$. Supposons que

$$(*) \qquad 0 = \mathrm{F}_1\ell_1 + \cdots + \mathrm{F}_n\ell_n,$$

avec $\mathrm{F}_i \in k(\widetilde{\mathrm{B}})$. En chassant les dénominateurs, on se ramène au cas où $\mathrm{F}_i \in k[\widetilde{\mathrm{B}}]$. On peut alors écrire chaque F_i comme une somme finie :

$$\mathrm{F}_i = \sum_{\nu\in\mathbb{N}^s} \mathrm{P}_{i,\nu}(b_1, \dots, b_t)c_1^{\nu_1} \cdots c_s^{\nu_s}.$$

Alors, $(*)$ entraîne, avec des notations évidentes,

$$0 = \sum_{\nu\in\mathbb{N}^s} \left(\sum_{i=1}^{n} \mathrm{P}_{i,\nu}(b)\ell_i \right) c^{\nu}.$$

D'après le lemme, on en déduit $\sum_{i=1}^{n} \mathrm{P}_{i,\nu}(b)\ell_i = 0$, pour tout ν, et comme les ℓ_i sont linéairement indépendants sur $k(\mathrm{B})$, il vient $\mathrm{P}_{i,\nu} = 0$ pour tout i, ν, et donc $\mathrm{F}_i = 0$ pour $i = 1, \dots, n$. Ceci montre que $\ell_1, \dots, \ell_n$ sont linéairement indépendants sur $k(\widetilde{\mathrm{B}})$. On en déduit que

$$[\mathrm{L} : k(\mathrm{B})] \leqslant [\mathrm{K} : k(\widetilde{\mathrm{B}})].$$

Or, $[\mathrm{K} : k(\widetilde{\mathrm{B}})] < \infty$, d'après le lemme 15.33. Donc L est une extension de degré fini, et a fortiori de type fini, de $k(\mathrm{B})$, et donc L est une extension de type fini de k. Ceci achève la preuve du théorème. □

VI. CORPS DE RUPTURE, CLÔTURES ALGÉBRIQUES, CORPS DE DÉCOMPOSITION

Séances des 13 et 14 novembre

16. Corps de rupture, clôtures algébriques

16.1. Corps de rupture d'un polynôme irréductible. —

Théorème 16.1 **(Corps de rupture d'un polynôme irréductible)**
Soient k un corps et $\mathrm{P} \in k[\mathrm{X}]$ un polynôme unitaire irréductible de degré $\geqslant 2$. Alors $\mathrm{K} := k[\mathrm{X}]/(\mathrm{P})$ est un surcorps de k dans lequel P a au moins une racine, à savoir l'image x de X. On l'appelle le **corps de rupture de P sur k.**

Le couple (K, x) vérifie la propriété universelle suivante : pour toute extension $k \subset \mathrm{L}$ telle que P admette dans L une racine α, il existe un **unique** *k-morphisme $\psi : \mathrm{K} \to \mathrm{L}$ tel que $\psi(x) = \alpha$; son image est le sous-corps $k[\alpha]$ de L. En particulier, ψ est un isomorphisme si $\mathrm{L} = k[\alpha]$.*

Démonstration. — On a déjà vu que (P) est un idéal maximal, donc K est un corps. Notant x l'image de X dans K, on a $\mathrm{P}(x) = 0$ et donc $x \in \mathrm{K}$ est bien une racine de P.

Soit $k \subset \mathrm{L}$ une extension telle que P admette dans L une racine α. Alors $\mathrm{Irr}_k(\alpha)$, le polynôme minimal de α sur k, divise P, donc lui est égal puisque P est irréductible et unitaire. Par conséquent, le morphisme de k-algèbres $\phi : k[\mathrm{X}] \to \mathrm{L}$ défini par $\phi(\mathrm{X}) = \alpha$ induit un morphisme $\psi : \mathrm{K} \to \mathrm{L}$ tel que $\psi(x) = \alpha$. De plus, ce morphisme est unique, puisque $\mathrm{K} = k[x]$ est engendré comme k-algèbre par x. Ceci prouve le théorème. □

(0) Version du 19/11/06

Exemple 16.2. — $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$. Plus généralement, montrez que pour tout binôme $P = X^2 + bX + c$ tel que $\Delta := b^2 - 4c$ soit < 0, le corps $\mathbb{R}[X]/(P)$ est isomorphe à $\mathbb{C}$.

Remarque 16.3. — L'exercice ci-dessus montre que des polynômes différents peuvent avoir des corps de rupture isomorphes.

Définition 16.4. — Soit $P \in k[X]$ irréductible. Il est commode de dire qu'une extension K de k est *un corps de rupture de* P *sur* k si $K \cong k[X]/(P)$.

Proposition 16.5. — *Soit* $K = k(\alpha)$ *une extension algébrique monogène et soient* $P = \mathrm{Irr}_k(\alpha)$ *et* $d = \deg P = \deg_k(\alpha)$. *Alors :*

1) K *est un corps de rupture de* P *sur* k.

2) *Pour toute extension* L/k, *le nombre de* k*-morphismes* $K \to L$ *est égal au nombre de racines de* P *dans* L. *Par conséquent, on a*

$$\#\,\mathrm{Hom}_{k\text{-}alg.}(K, L) \leqslant \deg P,$$

avec égalité si et seulement si P *a* d *racines distinctes dans* L.

Démonstration. — D'après le théorème, il existe un (unique) isomorphisme de $k[X]/(P)$ sur le sous-corps de K engendré par α, envoyant X sur α. Ceci prouve 1).

Pour tout k-morphisme $\phi : K \to L$, $\phi(\alpha)$ est une racine de P dans L. Réciproquement, comme $K \cong k[X]/(P)$, alors toute racine β de P dans L définit un morphisme de k-algèbres $\phi_\beta : K \to L$ tel que $\phi_\beta(\alpha) = \beta$, et évidemment ces morphismes sont deux à deux distincts. Ceci prouve 2). □

Exemple 16.6. — Soient $k = \mathbb{Q}$ et $P = X^3 - 2$. Alors P est irréductible sur $\mathbb{Q}$, car il n'a pas de racine dans $\mathbb{Q}$. Notons $\sqrt[3]{2}$ la racine cubique réelle de 2 et $j = \exp(2i\pi/3)$, $j^2 = \exp(4i\pi/3)$ les racines primitives de l'unité d'ordre 3 dans $\mathbb{C}$. Les racines de P dans $\mathbb{C}$ sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ et chacun des sous-corps suivants de $\mathbb{C}$:

$$\mathbb{Q}[\sqrt[3]{2}], \quad \mathbb{Q}[j\sqrt[3]{2}], \quad \mathbb{Q}[j^2\sqrt[3]{2}]$$

est un corps de rupture de P. Bien que $\mathbb{Q}$-isomorphes, ces trois sous-corps de $\mathbb{C}$ sont deux à deux distincts. En effet, $\mathbb{Q}[\sqrt[3]{2}]$ est contenu dans $\mathbb{R}$, donc distinct des deux autres. Si l'on avait $\mathbb{Q}[j\sqrt[3]{2}] = \mathbb{Q}[j^2\sqrt[3]{2}]$, alors ce corps, disons K, contiendrait j et donc $\sqrt[3]{2}$, donc contiendrait $\mathbb{Q}[\sqrt[3]{2}]$. Comme ces deux corps sont de même dimension $\deg P = 3$ sur $\mathbb{Q}$, on aurait $\mathbb{Q}[\sqrt[3]{2}] = K$, ce qui n'est pas le cas.

16.2. Corps algébriquement clos. —

***Définition 16.7* (Polynômes scindés).** — Soit K/k une extension de corps et soit $\mathrm{P} \in k[\mathrm{X}]$ non constant. On dit que P est **scindé dans** $\mathrm{K}[\mathrm{X}]$ (ou **sur** K), si P se décompose dans $\mathrm{K}[\mathrm{X}]$ comme produit de facteurs du premier degré, c.-à-d.,

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

où $d = \deg \mathrm{P}$, c est le coefficient dominant de P, et $\alpha_1, \ldots, \alpha_d$ sont les racines de P dans K, « comptées avec multiplicité » (par exemple, si $\mathrm{P} = (\mathrm{X} - \alpha)^d$ alors les racines sont $\alpha, \ldots, \alpha$ (d fois)).

***Définition 16.8*.** — Un corps K est dit **algébriquement clos** si tout $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ non constant a au moins une racine dans K.

***Lemme 16.9*.** — *Si* K *est algébriquement clos, tout* $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ *non constant est scindé.*

Démonstration. — 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 $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ de degré d. Comme K est algébriquement clos, P possède dans K au moins une racine α, donc se factorise en $\mathrm{P} = (\mathrm{X} - \alpha)\mathrm{Q}$, avec $\mathrm{Q} \in \mathrm{K}[\mathrm{X}]$ de degré $d - 1$. Par hypothèse de récurrence, Q est scindé dans $\mathrm{K}[\mathrm{X}]$, et donc il en est de même de P. □

***Définition 16.10*.** — Soit $k \subseteq \mathrm{K}$ une extension de corps. On dit que K est une **clôture algébrique de** k s'il vérifie les deux conditions suivantes :

a) K est algébriquement clos ;

b) K est **algébrique sur** k, c.-à-d., tout élément de K est algébrique sur k.

***Remarque 16.11*.** — On suppose connu du lecteur le fait que $\mathbb{C}$ est algébriquement clos (on en donnera une démonstration plus bas). Mais **attention**, $\mathbb{C}$ n'est **pas** algébrique sur $\mathbb{Q}$ car $\mathbb{C}$ contient des éléments qui ne sont pas algébriques sur $\mathbb{Q}$, par exemple π ou e.

***Théorème 16.12* (Steinitz).** — *Tout corps k admet une clôture algébrique, unique à k-isomorphisme (non-unique) près.*

Avant de démontrer ce théorème, établissons la proposition et le corollaire qui suivent.

***Proposition 16.13* (Fermeture algébrique de k dans K).** — *Soit* K/k *une extension de corps.* 1) *Alors :*

$$\mathrm{K}_{\mathrm{alg}/k} = \{x \in \mathrm{K} \mid x \text{ est algébrique sur } k\}$$

est un sous-corps de K*, appelé la fermeture algébrique de k dans* K.

2) *Supposons* K *algébriquement clos et posons* $\overline{k} = \mathrm{K}_{\mathrm{alg}/k}$. *Alors* $\overline{k}$ *est une clôture algébrique de* k.

Démonstration. — 1) Posons $\mathrm{K}' = \mathrm{K}_{\mathrm{alg}/k}$. Il est clair que $1 \in \mathrm{K}'$. Soient $x, y \in \mathrm{K}'$. Alors la sous-algèbre $k[x]$ est un corps, de degré $d = \deg_k(x)$ sur k. Comme y est algébrique sur k, il l'est aussi sur $k[x]$ et donc la sous-algèbre $k[x,y] = k[x][y]$ est un corps, égal à $k(x,y)$, et de degré $f = \deg_{k[x]}(y)$ sur $k[x]$. Donc,

$$[k(x,y) : k] = [k(x,y) : k(x)]\,[k(x) : k] = fd < \infty.$$

Comme $k(x,y)$ contient $x+y$ et xy, ces deux éléments sont algébriques sur k, c.-à-d., appartiennent à K'. Ceci montre que K' est un sous-corps de K.

2) D'après le point 1), $\overline{k}$ est un corps, algébrique sur k. Montrons que $\overline{k}$ est algébriquement clos. Soit $\mathrm{P} = a_0 + a_1\mathrm{X} + \cdots + a_d\mathrm{X}^d \in \overline{k}[\mathrm{X}]$, non constant. Comme les a_i sont algébriques sur k, le sous-corps $\mathrm{K} = k[a_0, \ldots, a_d]$ est de degré fini sur k, d'après le théorème 15.23.

D'autre part, comme L est algébriquement clos, il existe $\alpha \in \mathrm{L}$ tel que $\mathrm{P}(\alpha) = 0$. Alors α est algébrique sur K et donc sur k, d'après le théorème 15.23 à nouveau. Donc α appartient à $\overline{k}$. Ceci montre que $\overline{k}$ est algébriquement clos. La proposition est démontrée. □

Comme $\mathbb{C}$ est algébriquement clos, on obtient ainsi le corollaire suivant.

Corollaire 16.14. — *Le corps* $\overline{\mathbb{Q}} := \{z \in \mathbb{C} \mid z \text{ est algébrique sur } \mathbb{Q}\}$ *est une clôture algébrique de* $\mathbb{Q}$.

Démontrons maintenant le théorème de Steinitz. Désignons par

$$\{\mathrm{P}_\lambda \mid \lambda \in \Lambda\}$$

l'ensemble des polynômes irréductibles unitaires de $k[\mathrm{X}]$, et soit A la k-algèbre de polynômes en une infinité de variables X_λ, pour $\lambda \in \Lambda$. Pour tout $\lambda \in \Lambda$, soit

$$\mathrm{P}_\lambda(\mathrm{X}_\lambda)$$

l'image de P_λ dans A par le morphisme $k[\mathrm{X}] \to \mathrm{A}$ qui envoie X sur X_λ ; c.-à-d.,

$$\text{si } \mathrm{P}_\lambda = \mathrm{X}^d + \sum_{i=1}^{d} a_i\,\mathrm{X}^i, \qquad \text{alors } \mathrm{P}_\lambda(\mathrm{X}_\lambda) = \mathrm{X}_\lambda^d + \sum_{i=1}^{d} a_i\,\mathrm{X}_\lambda^i.$$

Notons I l'idéal de A engendré par les éléments $\mathrm{P}_\lambda(\mathrm{X}_\lambda)$, pour $\lambda \in \Lambda$.

Lemme 16.15. — I *est un idéal propre de* A.

Démonstration. — En effet, sinon il existerait un sous-ensemble fini $\Lambda_0 = \{\lambda_1, \ldots, \lambda_n\}$ de Λ tel que

$$1 = \sum_{i=1}^{n} \mathrm{Q}_i \mathrm{P}_{\lambda_i}(\mathrm{X}_{\lambda_i}), \qquad (*)$$

avec $\mathrm{Q}_i \in \mathrm{A}$. Désignons par Λ_1 la réunion de Λ_0 et des variables X_λ qui apparaissent dans $\mathrm{Q}_1, \ldots, \mathrm{Q}_n$; c'est un ensemble fini

$$\Lambda_1 = \{\lambda_1, \ldots, \lambda_n, \lambda_{n+1}, \ldots, \lambda_{\mathrm{N}}\},$$

et l'égalité $(*)$ a lieu dans l'anneau de polynômes $\mathrm{B} := k[\mathrm{X}_{\lambda_j} \mid j = 1, \ldots, \mathrm{N}]$, en un nombre fini de variables.

Soit k_1 un corps de rupture sur k du polynôme irréductible P_{λ_1} et soit α_1 une racine dans k_1 de P_{λ_1}.

Le polynôme P_{λ_2} n'est pas nécessairement irréductible sur k_1, mais peu importe : soit P_2 un facteur irréductible de P_{λ_2} dans $k_1[\mathrm{X}]$ et soit k_2 un corps de rupture sur k_1 de P_2. Alors

$$k \subset k_1 \subseteq k_2$$

et P_{λ_1} et P_{λ_2} ont une racine α_1, resp. α_2, dans k_2. Répétant ce processus, on obtient un surcorps k_n de k dans lequel chaque P_{λ_i} a une racine α_i, pour $i = 1, \ldots, n$. On peut alors considérer le morphisme

$$\phi : \mathrm{B} \longrightarrow k_n$$

défini par $\phi(\mathrm{X}_{\lambda_i}) = \alpha_i$, pour $i = 1, \ldots, n$ et $\phi(\mathrm{X}_j) = 0$ pour $j = n+1, \ldots, \mathrm{N}$, c.-à-d.,

$$\forall\, \mathrm{Q} \in \mathrm{B}, \qquad \phi(\mathrm{Q}) = \mathrm{Q}(\alpha_1, \ldots, \alpha_n, 0, \ldots, 0).$$

Alors, appliquant ϕ à l'égalité $(*)$, on obtient $1 = 0$, une contradiction. Cette contradiction montre que I est un idéal propre de A. Le lemme est démontré. □

Donc, puisque I est un idéal propre de A, il est contenu dans un idéal maximal $\mathfrak{m}$. Posons $\mathrm{K}_1 = \mathrm{A}/\mathfrak{m}$ et $\mathrm{K}_0 = k$. Pour tout $\lambda \in \Lambda$, notons x_λ l'image de X_λ dans K_1 ; c'est une racine du polynôme P_λ.

Proposition 16.16. — 1) *Tout polynôme irréductible de* $k[\mathrm{X}]$ *a une racine dans* K_1.

2) *De plus,* K_1 *est algébrique sur* $k = \mathrm{K}_0$.

Démonstration. — 1) est immédiat, car les polynômes irréductibles unitaires de $k[\mathrm{X}]$ sont les P_λ, et chacun a une racine x_λ dans K_1.

2) Soit $y \in \mathrm{K}_1$. Alors y est l'image dans K_1 d'un polynôme $\mathrm{Q} \in \mathrm{A}$ qui, nécessairement, ne fait intervenir qu'un nombre fini de variables X_{λ_i}, pour $i = 1, \ldots, s$. Donc y appartient à la sous-algèbre

$$\mathrm{C} := k[x_{\lambda_1}, \ldots, x_{\lambda_s}]$$

de K_1, et comme chaque x_{λ_i} est algébrique sur k (puisque racine du polynôme P_{λ_i}), on a $\dim_k \mathrm{C} < \infty$ et donc y est algébrique sur $k = \mathrm{K}_0$. La proposition est démontrée. □

Si K_1 n'est pas algébriquement clos, on peut appliquer à K_1 le même processus : on obtient ainsi une extension algébrique $\mathrm{K}_1 \subseteq \mathrm{K}_2$ dans laquelle tout polynôme irréductible de $\mathrm{K}_1[\mathrm{X}]$ a au moins une racine. On construit ainsi une suite croissante d'extensions algébriques :

$$k = \mathrm{K}_0 \subseteq \mathrm{K}_1 \subseteq \mathrm{K}_2 \subseteq \cdots$$

telle que tout polynôme irréductible $\mathrm{P} \in \mathrm{K}_i[\mathrm{X}]$ a une racine dans K_{i+1}. Alors

$$\mathrm{K} = \bigcup_{i \geqslant 0} \mathrm{K}_i$$

est un corps, algébrique sur $k = \mathrm{K}_0$, et algébriquement clos. En effet, tout polynôme irréductible $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ a tous ses coefficients dans un certain K_i, donc a une racine dans K_{i+1}, donc dans K. Ceci montre que k admet une clôture algébrique. (Cette démonstration est dûe à Emil Artin.)

Il reste à montrer l'unicité, à isomorphisme près. Commençons par le lemme ci-dessous.

Lemme 16.17. — *Soit $\tau : k \xrightarrow{\sim} k'$ un isomorphisme de corps. Il induit un isomorphisme d'anneaux*

$$\phi_\tau : k[\mathrm{X}] \xrightarrow{\sim} k'[\mathrm{X}], \qquad \sum_i a_i \mathrm{X}^i \mapsto \sum_i \tau(a_i)\mathrm{X}^i.$$

De plus, pour tout $\mathrm{P} \in k[\mathrm{X}]$, ϕ_τ induit un isomorphisme d'anneaux

$$k[\mathrm{X}]/(\mathrm{P}) \xrightarrow{\sim} k'[\mathrm{X}]/(\tau(\mathrm{P})).$$

Démonstration. — L'isomorphisme $\tau : k \xrightarrow{\sim} k'$ munit k', et donc aussi $k'[\mathrm{X}]$, d'une structure de k-algèbre. D'après la propriété universelle de $k[\mathrm{X}]$, il existe un unique morphisme de k-algèbres $\phi_\tau : k[\mathrm{X}] \to k'[\mathrm{X}]$ tel que $\phi_\tau(\mathrm{X}) = \mathrm{X}$, et ϕ_τ vérifie la formule donnée ci-dessus.

On obtient de même que l'isomorphisme $\tau^{-1} : k' \xrightarrow{\sim} k$ induit un morphisme

$$\phi_{\tau^{-1}} : k'[\mathrm{X}] \xrightarrow{\sim} k[\mathrm{X}], \qquad \sum_i a_i \mathrm{X}^i \mapsto \sum_i \tau^{-1}(a_i)\mathrm{X}^i,$$

et il est alors clair que ϕ_τ et $\phi_{\tau^{-1}}$ sont inverses l'un de l'autre. Ceci prouve la première assertion.

Enfin, pour tout $P \in k[X]$, il est clair que ϕ_τ et $\phi_{\tau^{-1}}$ induisent des bijections réciproques entre les idéaux (P) et $(\tau(P))$, et donc entre les anneaux quotients $k[X]/(P)$ et $k'[X]/(\tau(P))$. Ceci prouve le lemme. □

Théorème 16.18. — *Soient* K/k *une extension algébrique,* Ω *un corps algébriquement clos, et* $\tau : k \hookrightarrow \Omega$ *un morphisme de corps. Alors* τ *se prolonge à* K *(de façon non unique en général).*

Démonstration. — Soit E l'ensemble des couples (k', τ') où k'/k est une sous-extension de K/k et où τ' est un morphisme $k' \to \Omega$ prolongeant τ. Alors E est non vide, car il contient le couple (k, τ). On munit E de la relation d'ordre définie par :

$$(k', \tau') \leqslant (k'', \tau'') \Leftrightarrow k' \subseteq k'' \quad \text{et } \tau'' \text{ prolonge } \tau'.$$

Alors E est un ensemble ordonné **inductif**, i.e. tout sous-ensemble filtrant admet un majorant dans E. En effet, si $(k_i, \tau_i)_{i \in I}$ est une famille filtrante d'élements de E, alors

$$k' = \bigcup_{i \in I} k_i$$

est un sous-corps de K, et les τ_i se prolongent en un morphisme $\tau' : k' \to \Omega$ défini par $\tau'(x) = \tau_i(x)$ si $x \in k_i$. Ceci est bien défini, car si $x \in k_j$ avec $j \neq i$, il existe $\ell \in I$ tel que k_ℓ contienne k_i et k_j et alors

$$\tau_i(x) = \tau_\ell(x) = \tau_j(x).$$

Ceci montre que E est bien inductif, c.-à-d., vérifie l'hypothèse du théorème de Zorn (5.17, séances du 2-3 octobre). Donc, d'après le théorème de Zorn, E possède (au moins) un élément maximal (k_0, τ_0).

Montrons que $k_0 = K$. Soit $x \in K$. Alors x est algébrique sur k donc *a fortiori* sur k_0. Soit $P \in k_0[X]$ son polynôme minimal sur k_0. Alors le polynôme $\tau_0(P)$ a une racine α dans Ω, puisque Ω est algébriquement clos. Identifiant k_0 à son image dans Ω par τ_0, on obtient des isomorphismes

$$k_0[\alpha] \cong k_0[X]/(P) \cong k_0[x].$$

Par conséquent, τ_0 se prolonge en un morphisme

$$k_0[x] \xrightarrow{\sim} k_0[\alpha] \hookrightarrow \Omega.$$

Par maximalité de (k_0, τ_0), ceci entraîne $k_0 = k_0[x]$, d'où $x \in k_0$. Ceci montre que $k_0 = K$, et donc τ se prolonge en $\tau_0 : K \to \Omega$. Ceci prouve le théorème 16.18. □

Le dernier ingrédient pour achever la preuve du théorème de Steinitz est le résultat suivant, qui est intéressant en lui-même.

Lemme 16.19. — *Soit* L *une clôture algébrique de* k. *Alors* $k \subseteq \mathrm{L}$ *est une* **extension algébrique maximale**, *c.-à-d., si on a une extension*

$$k \subseteq \mathrm{L} \subseteq \mathrm{L}' \qquad \textit{avec } \mathrm{L}' \textit{ algébrique sur } k,$$

alors $\mathrm{L}' = \mathrm{L}$.

Démonstration. — Soit $x \in \mathrm{L}'$. Alors x est algébrique sur k donc *a fortiori* sur L. Soit P son polynôme minimal sur L. Comme L est algébriquement clos, P est de degré 1, c.-à-d., $x \in \mathrm{L}$. □

Corollaire 16.20. — *Soient* Ω, Ω' *deux clôtures algébriques de* k. *Alors il existe un* k*-isomorphisme* $\phi : \Omega \xrightarrow{\sim} \Omega'$.

Démonstration. — D'après le théorème 16.18 appliqué à $\mathrm{K} = \Omega'$, l'injection $\tau : k \hookrightarrow \Omega$ se prolonge en une injection

$$k \hookrightarrow \Omega' \overset{\tau'}{\hookrightarrow} \Omega.$$

Alors, comme Ω' est algébriquement clos et Ω/k algébrique, l'injection τ' est surjective, c.-à-d., c'est un k-isomorphisme $\Omega' \xrightarrow{\sim} \Omega$. Ceci prouve le corollaire et achève la preuve du théorème de Steinitz 16.12. □

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

Théorème 16.21. — $\mathbb{C}$ *est algébriquement clos, c.-à-d., tout polynôme* $\mathrm{P} \in \mathbb{C}[\mathrm{X}]$, *non constant, admet une racine dans* $\mathbb{C}$.

Remarque 16.22. — 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).

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].

Voici donc 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

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

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

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

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 $e^{i\pi} = -1$, alors

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

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

$$\forall\, \varepsilon \leqslant \varepsilon_0, \qquad |h(\varepsilon)| \leqslant \frac{r}{2}.$$

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.

17. Corps de décomposition d'un polynôme

Définition 17.1. — Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme non constant. On dit qu'une extension K de k est un **corps de décomposition de** P **sur** k si elle vérifie les deux conditions suivantes :

1) P a toutes ses racines dans K, c.-à-d., est scindé dans K[X].

2) K est engendré sur k par les racines de P. (Ceci entraîne que K est de degré fini sur k, d'après la proposition 15.23.)

Théorème 17.2 **(Corps de décomposition d'un polynôme)**
Tout $\mathrm{P} \in k[\mathrm{X}]$ *non constant admet un corps de décomposition sur* k*, unique à* k*-isomorphisme près.*

Démonstration. — Soit Ω une clôture algébrique de k, soient $\alpha_1, \ldots, \alpha_n$ les racines de P de Ω et soit K_0 le sous-corps de Ω engendré par les α_i. Il est clair que K_0 est un corps de décomposition de P sur k.

Pour montrer l'unicité à isomorphisme près, on va établir le résultat plus précis suivant. (Le cas particulier $k = k'$ et $\tau = \mathrm{id}_k$ fournit l'unicité à isomorphisme près du corps de décomposition.) On rappelle le lemme 16.17.

Théorème 17.3 **(Unicité du corps de décomposition)**. — *Soient* $\tau : k \xrightarrow{\sim} k'$ *un isomorphisme de corps,* $\mathrm{P} \in k[\mathrm{X}]$ *non constant et* K*, resp.* K′*, un corps de décomposition de* P *sur* k*, resp. de* $\tau(\mathrm{P})$ *sur* k'*. Alors* τ *se prolonge en un isomorphisme* $\sigma : \mathrm{K} \xrightarrow{\sim} \mathrm{K}'$*.*

Démonstration. — Posons $\mathrm{P}' = \tau(\mathrm{P})$ et soient $\beta_1, \ldots, \beta_n$ les racines de P′ dans K′. Soit Ω une clôture algébrique de k. Traitons d'abord le cas où $\mathrm{K} = \mathrm{K}_0$ est le sous-corps de Ω engendré par les racines $\alpha_1, \ldots, \alpha_n$ de P de Ω.

Comme l'extension $k \xrightarrow{\sim} k' \subseteq \mathrm{K}'$ est algébrique alors, d'après le théorème 16.18, l'injection $k \hookrightarrow \Omega$ se prolonge en une injection

$$\phi : \mathrm{K}' \hookrightarrow \Omega,$$

telle que $\phi(\mathrm{P}') = \phi(\tau(\mathrm{P})) = \mathrm{P}$. Par conséquent, les racines β_i de P′ dans K′ sont envoyées par ϕ sur les racines de P dans Ω, et comme K′ est engendré sur k' par les β_i, alors $\phi(\mathrm{K}')$ est engendré sur $\phi(k') = k$ par les α_i, et donc $\phi(\mathrm{K}') = \mathrm{K}_0$. Ceci prouve le résultat voulu pour $\mathrm{K} = \mathrm{K}_0$.

Enfin, pour K arbitraire, le même raisonnement fournit un k-isomorphisme $\psi : \mathrm{K} \xrightarrow{\sim} \mathrm{K}_0$. Alors,

$$\phi^{-1} \circ \psi : \mathrm{K} \xrightarrow{\sim} \mathrm{K}'$$

est un isomorphisme prolongeant τ. Ceci prouve le théorème 17.3 et achève la preuve du théorème 17.2. □

□

Remarque 17.4. — Voici une **autre démonstration** des deux théorèmes précédents, qui est « constructive » et n'utilise pas les résultats portant sur la clôture algébrique.

1) On va démontrer **l'existence** d'un corps de décomposition de P sur k par récurrence sur $n = \deg \mathrm{P}$. Si $n = 1$, alors $\mathrm{P} = a\mathrm{X} - b = a(\mathrm{X} - b/a)$ et k est un corps de décomposition de P. Supposons $n \geqslant 2$ et le théorème établi pour tout corps et tout polynôme de degré $< n$, et soit $\mathrm{P} \in k[\mathrm{X}]$ de degré n.

Soit S un facteur irréductible de P et soit $k_1 = k(\alpha)$ un corps de rupture de S. Alors, dans $k_1[\mathrm{X}]$, on a $\mathrm{P} = (\mathrm{X} - \alpha)\mathrm{Q}$, avec $\mathrm{Q} \in k_1[\mathrm{X}]$ de degré $n - 1$. Par hypothèse de récurrence, il existe une extension K/k_1 dans laquelle Q a des racines $\alpha_2, \ldots, \alpha_n$ et telle que $\mathrm{K} = k_1(\alpha_2, \ldots, \alpha_n)$. Alors, $\alpha, \alpha_2, \ldots, \alpha_n$ sont les racines de P dans K, et K est engendré sur k par ces élements. Ceci montre l'existence d'un corps de décomposition.

Démontrons maintenant **l'unicité**, sous la forme plus forte donnée dans le théorème 17.3.

On procède par récurrence sur le **nombre** m **de racines de** P **qui sont dans** K **mais pas dans** k. Sans perte de généralité, on peut supposer P unitaire. Si $m = 0$, alors

$$\mathrm{P} = (\mathrm{X} - \lambda_1) \cdots (\mathrm{X} - \lambda_n),$$

avec les λ_i dans k. Dans ce cas, $\mathrm{K} = k$ et

$$\tau(\mathrm{P}) = (\mathrm{X} - \tau(\lambda_1)) \cdots (\mathrm{X} - \tau(\lambda_n)),$$

avec $\tau(\lambda_i) \in k'$, donc $\mathrm{K}' = k'$ et l'on peut prendre $\sigma = \tau$.

Supposons $m > 0$ et le théorème établi pour tout $m' < m$. Soit $\mathrm{P} \in k[\mathrm{X}]$ ayant exactement m racines dans $\mathrm{K} \setminus k$, et soit

$$\mathrm{P} = \mathrm{P}_1 \cdots \mathrm{P}_r \tag{1}$$

sa décomposition en facteurs irréductibles dans $k[\mathrm{X}]$. Comme $m > 0$, l'un au moins de ces facteurs, disons P_1, est de degré $\geqslant 2$ et n'a pas de racines dans k.

Par hypothèse, P se scinde dans K[X] comme produit de facteurs (irréductibles !) de degré 1. Comme K[X] est **factoriel**, l'unicité d'une telle décomposition entraîne que chaque P_i est un produit de certains de ces facteurs linéaires.

En particulier, P_1 a toutes ses racines dans K. Soit α l'une d'elles. D'après la proposition 16.5, on a un k-isomorphisme

$$\psi : k[\mathrm{X}]/(\mathrm{P}_1) \xrightarrow{\sim} k[\alpha]. \tag{2}$$

D'autre part,

$$\tau(\mathrm{P}) = \tau(\mathrm{P}_1)\cdots\tau(\mathrm{P}_r), \tag{1'}$$

et, par le même argument que précédemment, chaque $\tau(\mathrm{P}_i)$ a toutes ses racines dans K$'$. Soit β une racine de $\tau(\mathrm{P}_1)$ dans K$'$. D'après la proposition 16.5, à nouveau, on a un k'-isomorphisme

$$\psi' : k'[\mathrm{X}]/(\tau(\mathrm{P}_1)) \xrightarrow{\sim} k'[\beta]. \tag{2'}$$

De plus, d'après le lemme 16.17, on a un isomorphisme

$$\phi_\tau : k[\mathrm{X}]/(\mathrm{P}_1) \xrightarrow{\sim} k'[\mathrm{X}]/(\tau(\mathrm{P}_1))$$

qui prolonge $\tau : k \xrightarrow{\sim} k'$. Posons $k_1 = k[\alpha]$ et $k_1' = k'[\beta]$. Alors, $\tau_1 := \psi' \circ \phi_\tau \circ \psi^{-1}$ est un isomorphisme $k_1 \xrightarrow{\sim} k_1'$ qui prolonge τ. On a donc le diagramme suivant :

$$\begin{array}{ccccc} k & \subset & k_1 & \subset & \mathrm{K} \\ {\scriptstyle\tau}\downarrow & \cong & {\scriptstyle\tau_1}\downarrow & \cong & \\ k' & \subset & k_1' & \subset & \mathrm{K}'. \end{array}$$

Maintenant, K (resp. K$'$) est un corps de décomposition sur k_1 (resp. sur k_1') de notre polynôme P (resp. de $\tau(\mathrm{P})$), et le nombre de racines de P dans $\mathrm{K} \setminus k_1$ est $< m$. Donc, par hypothèse de récurrence, il existe un isomorphisme $\sigma : \mathrm{K} \xrightarrow{\sim} \mathrm{K}'$ tel que $\sigma|_{k_1} = \tau_1$. Par conséquent, $\sigma|_k = \tau_1|_k = \tau$. Ceci achève la preuve de l'unicité.

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.