

Maîtrise de mathématiques

Cours de Calcul algébrique

2011–2012

Luis Paris

Partie 1 : Les polynômes

1 Définitions et propriétés de base

Définition. Soit A un anneau commutatif. L'ensemble des polynômes (à une variable) à coefficients dans A , noté $A[X]$, est l'ensemble des applications $f : \mathbb{N} \rightarrow A$ qui valent 0 sauf un nombre fini d'éléments de \mathbb{N} .

Définition. Soient $a \in A$ et $n \in \mathbb{N}$. On note aX^n le polynôme

$$aX^n : \mathbb{N} \rightarrow A \\ k \mapsto \begin{cases} 0 & \text{si } k \neq n \\ a & \text{si } k = n \end{cases}$$

On observe que tout polynôme $f \in A[X]$ s'écrit sous la forme

$$f = a_0X^0 + a_1X + \cdots + a_nX^n,$$

où $n \in \mathbb{N}$ et $a_i \in A$ pour tout $i \in \{0, 1, \dots, n\}$. Le terme a_i s'appelle le i -ème coefficient de f .

Définition. On définit la somme et la multiplication dans $A[X]$ comme suit. Soient $f = \sum_{i=0}^n a_iX^i$ et $g = \sum_{j=0}^m b_jX^j$. Alors

$$f + g = \sum_{i=0}^{\text{Sup}(n,m)} (a_i + b_i)X^i, \quad f \cdot g = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i + b_j \right) X^k.$$

Proposition 1.1.

- (1) $A[X]$ muni de la somme et la multiplication est un anneau commutatif.
- (2) L'application

$$A \rightarrow A[X] \\ a \mapsto aX^0$$

est un homomorphisme injectif.

Démonstration. Exercice. □

Définition. Soient A un sous-anneau d'un anneau B et $f = \sum_{i=0}^n a_i X^i \in A[X]$. L'application polynomiale à valeurs dans B associée à f est l'application

$$\begin{aligned} f_B : B &\rightarrow B \\ b &\mapsto \sum_{i=0}^n a_i b^i \end{aligned}$$

Définition. Soient A un sous-anneau d'un anneau B et $b \in B$. L'application

$$\begin{aligned} \text{ev}_B : A[X] &\rightarrow B \\ f &\mapsto f_B(b) \end{aligned}$$

s'appelle *l'homomorphisme d'évaluation*. C'est un homomorphisme (comme son nom l'indique). L'image de ev_B se note $A[b]$. C'est le sous-anneau de B engendré par $A \cup \{b\}$. On dit que b est *transcendant* sur A si ev_B est injectif.

Exemple 1. $\sqrt{2}$ n'est pas transcendant sur \mathbb{Z} car, si $f = X^2 - 2$, alors $f(\sqrt{2}) = 0$. L'anneau $\mathbb{Z}[\sqrt{2}]$ est formé des nombres de la forme $a\sqrt{2} + b$ avec $a, b \in \mathbb{Z}$ (exercice).

Exemple 2. Soit \mathbb{K} un corps fini. Il existe un polynôme non nul sur \mathbb{K} dont la fonction polynomiale sur \mathbb{K} est nulle.

Définition. Soient A un anneau commutatif et

$$f = a_0 + a_1 X + \cdots + a_n X^n, \quad a_n \neq 0,$$

un polynôme non nul. Le nombre n s'appelle le *degré* de f et se note $n = \deg f$. Le coefficient a_n s'appelle le *coefficient dominant* et se note $a_n = \text{cd}(f)$. Par convention, le degré du polynôme nul est $-\infty$. Un *polynôme constant* est un polynôme de degré 0 ou nul. Un *polynôme linéaire* est un polynôme de degré 1.

Définition. Soit A un anneau. Un élément $a \in A \setminus \{0\}$ est un *diviseur de zéro* s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$. On dit que A est *intègre* s'il n'a pas de diviseur de zéro.

Proposition 1.2. Soient A un anneau intègre et $f, g \in A[X]$. Alors

$$\deg(f + g) \leq \max\{\deg f, \deg g\}, \quad \deg(f \cdot g) = \deg f + \deg g.$$

Démonstration. Exercice. □

Corollaire 1.3. Si A est intègre alors $A[X]$ l'est aussi.

Démonstration. Exercice. □

Théorème 1.4 (Théorème d'Euclide). Soient A un anneau commutatif et $f, g \in A[X]$ tels que $g \neq 0$ et $\text{cd}(g)$ est inversible dans A . Alors il existe des polynômes $q, r \in A[X]$ uniques tels que

$$f = qg + r, \quad \deg r < \deg g.$$

Définition. L'expression $f = qg + r$ s'appelle la *division de f par g* , q est le *quotient* et r le *reste* de la division.

Démonstration. Existence : Si $f = 0$, alors on pose $q = r = 0$ et on a bien $f = qg + r$ et $\deg r = -\infty < \deg g$. On peut donc supposer que $f \neq 0$.

On pose

$$f = a_0 + a_1X + \cdots + a_nX^n, \quad g = b_0 + b_1X + \cdots + b_dX^d,$$

où $a_n \neq 0$ et $b_d \neq 0$. En particulier, $\deg f = n$, $\deg g = d$ et b_d^{-1} existe. On va démontrer l'existence de q et r par récurrence sur n .

Supposons que $n = 0$. Si $d = 0$, on pose $q = a_0b_0^{-1}$ et $r = 0$, et on a bien $f = qg + r$ et $\deg r = -\infty < 0 = \deg g$. Si $d > 0$, on pose $q = 0$ et $r = f$, et on a bien $f = qg + r$ et $\deg r = 0 < d = \deg g$.

On suppose que $n > 0$ plus l'hypothèse de récurrence. Si $n < d$ on pose $q = 0$ et $r = f$, et on a bien $f = qg + r$ et $\deg r = n < d = \deg g$. On peut donc supposer que $n \geq d$. Soit

$$f_1 = f - b_d^{-1}a_nX^{n-d}g.$$

On observe que $\deg f_1 < \deg f$. Par hypothèse de récurrence, il existe $q_1, r \in A[X]$ tels que $f_1 = q_1g + r$ et $\deg r < \deg g$. Soit

$$q = q_1 + b_d^{-1}a_nX^{n-d}.$$

Alors

$$f = f_1 + b_d^{-1}a_nX^{n-d}g = q_1g + r + b_d^{-1}a_nX^{n-d}g = (q_1 + b_d^{-1}a_nX^{n-d})g + r = qg + r,$$

et $\deg r < \deg g$.

Unicité : Observons d'abord que, si h_1, h_2 sont deux polynômes non nuls et le coefficient dominant de h_1 est inversible, alors

$$\deg(h_1h_2) = \deg(h_1) + \deg(h_2).$$

Supposons donnés $q_1, q_2, r_1, r_2 \in A[X]$ tels que

$$f = q_1g + r_1 = q_2g + r_2, \quad \deg r_1, \deg r_2 < \deg g.$$

On a

$$(q_1 - q_2)g = r_2 - r_1$$

donc

$$\deg(q_1 - q_2) + \deg g = \deg(r_2 - r_1).$$

Par ailleurs

$$\deg(r_2 - r_1) \leq \max\{\deg r_1, \deg r_2\} < \deg g.$$

Ceci n'est possible que si $q_1 - q_2 = 0$, c'est-à-dire $q_1 = q_2$. Il s'en suit aussi que $r_1 = r_2$. \square

Définition. On dit qu'un anneau A est *principal* s'il est intègre et si tout idéal de A est *monogène* (i.e. engendré par un seul élément).

Théorème 1.5. Si \mathbb{K} est un corps, alors $\mathbb{K}[X]$ est un anneau principal.

Démonstration. On sait déjà que $\mathbb{K}[X]$ est intègre. Soit I un idéal non nul de $\mathbb{K}[X]$. Posons

$$d = \min\{\deg f \mid f \in I \setminus \{0\}\}.$$

Soit $f_0 \in I$ tel que $\deg f_0 = d$. On va montrer que $I = (f_0)$.

Comme $f_0 \in I$ on a $(f_0) \subset I$. Montrons que $I \subset (f_0)$. Soit $f \in I$. Soit $f = qf_0 + r$ la division de f par f_0 . On a $r = f - qf_0 \in I$. Par ailleurs $\deg r < \deg f_0 = d$. Par la minimalité de d , on en conclue que $r = 0$, donc $f = qf_0 \in (f_0)$. \square

Définition. Soient A un anneau et $a \in A$. On dit que a est une *unité* s'il existe $b \in A$ tel que $ab = 1$. L'ensemble des unités de A est un groupe noté $U(A)$. Un élément $a \in A$ est *irréductible* si $a \notin U(A)$ et, si $a = a_1a_2$, alors $a_1 \in U(A)$ ou $a_2 \in U(A)$. On dit que A est *factoriel* si

(a) tout $a \in A \setminus \{0\}$ s'écrit sous la forme

$$a = ux_1x_2 \cdots x_n,$$

avec $u \in U(A)$ et x_1, \dots, x_n irréductibles ;

(b) si, pour $a \in A \setminus \{0\}$, on a

$$a = ux_1x_2 \cdots x_p = vy_1y_2 \cdots y_q,$$

où $u, v \in U(A)$ et $x_1, \dots, x_p, y_1, \dots, y_q$ sont irréductibles, alors $p = q$ et, à permutation près,

$$x_i = w_iy_i,$$

où $w_i \in U(A)$ pour tout $i \in \{1, \dots, p\}$.

Théorème 1.6. *Tout anneau principal est factoriel.*

Démonstration. Exercice. □

Corollaire 1.7. *Si \mathbb{K} est un corps, alors $\mathbb{K}[X]$ est un anneau factoriel.*

Lemme 1.8. *Soit A un anneau intègre. Alors $U(A[X]) = U(A)$.*

Démonstration. Exercice. □

Définition. Soient A, B deux anneaux tels que $A \subset B$ et $f \in A[X]$. On dit que $b \in B$ est une *racine* de f si $f_B(b) = 0$.

Théorème 1.9. *Soient A un anneau intègre et $f \in A[X]$ un polynôme non nul de degré $d \geq 0$.*

(1) *f a au plus d racines.*

(2) *Si $a \in A$ est une racine de f , alors $(X - a)$ divise f .*

Démonstration. Soit a une racine de f . Soit $f = q(X - a) + r$ la division de f par $(X - a)$. On a $\deg r < \deg(X - a) = 1$, donc r est un polynôme constant, c'est-à-dire qu'il existe $b \in A$ tel que $r = b$. On a

$$0 = f(a) = q(a) \cdot (a - a) + b = b,$$

d'où $f = q(X - a)$. Donc, $(X - a)$ divise f .

On démontre par récurrence sur $\deg f$ que f a au plus $\deg f$ racines. Si $\deg f = 0$, alors il existe $b \in A \setminus \{0\}$ tel que $f = b$. Si $a \in A$, alors $f(a) = b \neq 0$, donc f n'a pas de racine.

Supposons que $\deg f > 0$ plus l'hypothèse de récurrence. Si f n'a pas de racine, alors le nombre de racines est trivialement inférieur au degré de f . On peut donc supposer que f a une racine, a_0 . Par ce qui précède, il existe $g \in A[X]$ tel que $f = g(X - a_0)$. On a

$$\deg f = \deg g + \deg(X - a_0) = \deg g + 1,$$

c'est-à-dire $\deg g = \deg f - 1$. Par ailleurs, si a est une racine de f différente de a_0 alors

$$0 = f(a) = g(a) \cdot (a - a_0),$$

donc $g(a) = 0$ car A est intègre et $a - a_0 \neq 0$. En d'autres termes, l'ensemble des racines de f est la réunion de l'ensemble de racines de g avec $\{a_0\}$. Comme, par hypothèse de récurrence, g a au plus $\deg g$ racines, on en conclue que f a au plus $\deg g + 1 = \deg f$ racines. □

Corollaire 1.10. Soient A un anneau intègre, $T \subset A$ une partie infinie, et $f \in A[X]$ un polynôme tel que $f(x) = 0$ pour tout $x \in T$. Alors $f = 0$. \square

Corollaire 1.11. Soient A un anneau intègre, $T \subset A$ une partie infinie, et $f \in A[X_1, \dots, X_n]$. Si f s'annule sur T^n , alors f est nul.

Démonstration. Exercice. \square

Corollaire 1.12. Soient $n \in \mathbb{N}$, $n \geq 1$, A un anneau intègre infini, et $\mathcal{F}(A^n, A)$ l'anneau des applications de A^n dans A . Alors l'application $\varphi : A[X_1, \dots, X_n] \rightarrow \mathcal{F}(A^n, A)$, qui à un polynôme associe sa fonction polynomiale, est un homomorphisme injectif. \square

Lemme 1.13. Soit G un groupe abélien fini. Si G n'est pas cyclique, alors il existe un sous-groupe H de G et un nombre premier $p \geq 2$ tel que H soit isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Démonstration. Exercice. \square

Théorème 1.14. Soient A un anneau intègre et G un sous-groupe fini de $U(A)$. Alors G est cyclique.

Démonstration. Soit G un sous-groupe de $U(A)$. Supposons que G n'est pas cyclique. Par le lemme 1.13 il existe un nombre premier $p \geq 2$ et un sous-groupe H de G tel que H soit isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. On observe que $|H| = p^2$ et tout élément $a \in H$ vérifie $a^p = 1$, c'est-à-dire tout élément $a \in H$ est racine de $f = X^p - 1$. Or, par le théorème 1.9, f ne peut pas avoir plus de p racines, ce qui est contradictoire car $|H| = p^2 > p$. On en conclue que G est cyclique. \square

Corollaire 1.15. Soit \mathbb{K} un corps fini. Alors \mathbb{K}^* est un groupe cyclique.

Définition. Soit \mathbb{K} un corps. Soient $x \in \mathbb{K}^*$ et $n \in \mathbb{N}$, $n \geq 2$. On dit que x est une racine n -ème de l'unité si $x^n = 1$. On note $\mu_n(\mathbb{K})$ l'ensemble de toutes les racines n -èmes de l'unité et $\mu(\mathbb{K}) = \bigcup_{n=2}^{\infty} \mu_n(\mathbb{K})$.

Lemme 1.16. Soit \mathbb{K} un corps.

- (1) $\mu(\mathbb{K})$ est un sous-groupe de \mathbb{K}^* .
- (2) $\mu_n(\mathbb{K})$ est un sous-groupe cyclique de \mathbb{K}^* d'ordre au plus n .

Démonstration. Exercice. \square

Définition. Soient \mathbb{K} un corps et $n \in \mathbb{N}$, $n \geq 2$. Un générateur de $\mu_n(\mathbb{K})$ s'appelle une racine primitive n -ème de l'unité.

Définition. On dit qu'un corps \mathbb{K} est algébriquement clos si tout polynôme non constant à coefficients dans \mathbb{K} a une racine dans \mathbb{K} .

Lemme 1.17. Soit \mathbb{K} un corps algébriquement clos. Alors un polynôme $f \in \mathbb{K}[X]$ est irréductible si et seulement s'il est de degré 1.

Démonstration. Par le lemme 1.8 on a $U(\mathbb{K}[X]) = U(\mathbb{K}) = \mathbb{K}^*$, donc les polynômes irréductibles sont de degré ≥ 1 (il ne peuvent être ni 0, ni des unités). Si $f \in \mathbb{K}[X]$ est de degré 1 et $f = f_1 f_2$, alors

$$1 = \deg f = \deg f_1 + \deg f_2,$$

donc $\deg f_1 = 0$ ou $\deg f_2 = 0$, donc $f_1 \in \mathbb{K}^* = U(\mathbb{K}[X])$ ou $f_2 \in \mathbb{K}^* U(\mathbb{K}[X])$. Ceci montre que f est irréductible. Réciproquement, soit $f \in \mathbb{K}[X]$ un polynôme irréductible. Rappelons que, par ce qui précède, $\deg f \geq 1$. Par définition, f admet une racine, $a \in \mathbb{K}$. Par le théorème 1.9, $(X - a)$ divise f , donc, comme f est irréductible, f est de la forme $f = b(X - a)$ avec $b \in U(\mathbb{K}[X]) = \mathbb{K}^*$. En particulier f est de degré 1. \square

Corollaire 1.18. Soit \mathbb{K} un corps algébriquement clos. Alors tout polynôme non constant $f \in \mathbb{K}[X]$ se factorise sous la forme

$$f = c(X - a_1)^{m_1}(X - a_2)^{m_2} \cdots (X - a_d)^{m_d},$$

où a_1, \dots, a_d sont les racines de f , $m_i \geq 1$ pour tout $i \in \{1, \dots, d\}$ et $m_1 + \dots + m_d = \deg f$. \square

Définition. Soient A un anneau commutatif et

$$f = a_0 + a_1 X + \cdots + a_n X^n \in A[X].$$

Le polynôme dérivé de f est

$$f' = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

Lemme 1.19. Soient $f, g \in A[X]$ et $a \in A$. Alors

$$(f + g)' = f' + g', \quad (fg)' = f' \cdot g + f \cdot g', \quad (af)' = a f'.$$

Démonstration. Exercice. \square

Définition. Soient \mathbb{K} un corps, $f \in \mathbb{K}[X]$ un polynôme non constant, et $a \in \mathbb{K}$ une racine de f . On peut écrire f sous la forme

$$f = g(X - a)^m,$$

où $g \in \mathbb{K}[X]$ est tel que $g(a) \neq 0$, et $m \geq 1$. Le nombre m s'appelle la *multiplicité* de la racine a . Si $m \geq 2$, on dit que a est une *racine multiple*.

Proposition 1.20. Soient \mathbb{K} un corps, $f \in \mathbb{K}[X]$ un polynôme non constant, et $a \in \mathbb{K}$ une racine de f . Alors a est racine multiple si et seulement si $f'(a) = 0$.

Démonstration. On écrit f sous la forme $f = g(X - a)^m$ où $g \in \mathbb{K}[X]$ est tel que $g(a) \neq 0$, et $m \geq 1$. Supposons que $m = 1$. Alors

$$f' = g + g'(X - a)$$

donc

$$f'(a) = g(a) + g'(a)(a - a) = g(a) \neq 0.$$

Supposons que $m \geq 2$. Alors

$$f' = m g(X - a)^{m-1} + g'(X - a)^m,$$

donc

$$f'(a) = m g(a)(a - a)^{m-1} + g'(a)(a - a)^m = 0.$$

□

Définition. Soit \mathbb{K} un corps. L'homomorphisme $c : \mathbb{Z} \rightarrow \mathbb{K}$ défini par $c(m) = m 1_{\mathbb{K}}$ s'appelle l'homomorphisme caractéristique de \mathbb{K} .

Lemme 1.21. Soient \mathbb{K} un corps et $c : \mathbb{Z} \rightarrow \mathbb{K}$ l'homomorphisme caractéristique de \mathbb{K} . Soit $\text{Ker } c = \{0\}$, soit il existe un nombre premier $p \geq 2$ tel que $\text{Ker } c = p\mathbb{Z}$.

Démonstration. Exercice. □

Définition. Soient \mathbb{K} un corps et $c : \mathbb{Z} \rightarrow \mathbb{K}$ l'homomorphisme caractéristique. On dit que \mathbb{K} est de caractéristique 0 si $\text{Ker } c = \{0\}$ et on dit que \mathbb{K} est de caractéristique p si $\text{Ker } c = p\mathbb{Z}$, où p est un nombre premier.

Théorème 1.22. Soit \mathbb{K} un corps.

- (1) \mathbb{K} est de caractéristique 0 si et seulement s'il contient un sous-corps isomorphe à \mathbb{Q} .
- (2) \mathbb{K} est de caractéristique p si et seulement s'il contient un sous-corps isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Démonstration. Exercice. □

Lemme 1.23. Soient p un nombre premier, \mathbb{K} un corps de caractéristique p , et $a, b \in \mathbb{K}$. Alors

$$(a + b)^p = a^p + b^p, \quad (ab)^p = a^p b^p.$$

Démonstration. L'égalité $(ab)^p = a^p b^p$ est évidente, donc on doit juste démontrer $(a + b)^p = a^p + b^p$.

Soit $k \in \{1, \dots, p - 1\}$. Rappelons que

$$C_p^k = \frac{p!}{k!(p-k)!}.$$

Comme p ne divise aucun élément de $\{1, \dots, p - k\}$, p ne divise pas $(p - k)!$. De même, p ne divise pas $k!$. Comme p divise $p!$, on en déduit que p divise C_p^k . Il s'en suit que

$$C_p^k 1_{\mathbb{K}} = 0_{\mathbb{K}},$$

donc

$$C_p^k x = (C_p^k 1_{\mathbb{K}}) x = 0_{\mathbb{K}} x = 0_{\mathbb{K}}$$

pour tout $x \in \mathbb{K}$. Finalement

$$(a + b)^p = \sum_{k=0}^p C_p^k a^{p-k} b^k = a^p + b^p.$$

□

Corollaire 1.24. Soit \mathbb{K} un corps de caractéristique $p \geq 2$. Alors l'application

$$\begin{aligned} \varphi : \mathbb{K} &\rightarrow \mathbb{K} \\ x &\mapsto x^p \end{aligned}$$

est un endomorphisme.

□

Définition. L'endomorphisme du Corollaire 1.24 s'appelle *l'endomorphisme de Froebenius*.

Lemme 1.25.

- (1) Soient \mathbb{K} un corps et A un anneau. Alors tout homomorphisme $\mathbb{K} \rightarrow A$ est injectif.
- (2) Si \mathbb{K} est un corps fini, alors tout endomorphisme $\mathbb{K} \rightarrow \mathbb{K}$ est un automorphisme.

Démonstration. Exercice.

□

Corollaire 1.26. Soit \mathbb{K} un corps de caractéristique $p \geq 2$. Alors l'endomorphisme de Froebenius $\varphi : \mathbb{K} \rightarrow \mathbb{K}$ est injectif. C'est un automorphisme si \mathbb{K} est fini.

□

Corollaire 1.27. Soient \mathbb{K} un corps de caractéristique $p \geq 2$ et $a \in \mathbb{K}$. Alors, pour tout $r \in \mathbb{N}$,

$$X^{p^r} - a^{p^r} = (X - a)^{p^r}.$$

□

Exemple. Soit \mathbb{K} un corps de caractéristique $p \geq 2$. Alors, pour $r \in \mathbb{N}$,

$$X^{p^r} - 1 = (X - 1)^{p^r}.$$

En particulier, il existe une unique racine p^r -ème de l'unité dans $\mathbb{K} : 1$.

2 Polynômes à coefficients dans un anneau factoriel

Définition. Soit A un anneau intègre. Un élément $a \in A$ est *irréductible* s'il n'est ni nul, ni inversible, ni produit de deux éléments non inversibles. Il est *premier* s'il n'est ni nul ni inversible et si, pour tout produit $b_1 b_2$ divisible par a , l'un des deux facteurs b_1 ou b_2 est divisible par a .

Lemme 2.1. Soient A un anneau intègre et $a \in A$.

- (1) Si a est premier, alors a est irréductible.
- (2) Supposons que A soit factoriel. Alors a est premier si et seulement s'il est irréductible.

Démonstration. Exercice. □

Théorème 2.2. Soit A un anneau intègre. Il existe un corps \mathbb{K} , unique à isomorphisme près, tel que

- (a) A s'identifie à un sous-anneau de \mathbb{K} ;
- (b) Pour tout $x \in \mathbb{K}$ il existe $a \in A \setminus \{0\}$ tel que $ax \in A$.

Démonstration. Soit \sim la relation dans $A \times A \setminus \{0\}$ définie par

$$(a, b) \sim (a', b') \text{ si } ab' = a'b.$$

On vérifie facilement que \sim est une relation d'équivalence et on note \mathbb{K} l'ensemble des classes d'équivalence. Par ailleurs, la classe d'une paire (a, b) sera notée $\frac{a}{b}$.

On définit une somme et une multiplication dans \mathbb{K} par

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}, \quad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}.$$

Montrons que ces opérations sont bien définies. Supposons que $\frac{a_1}{b_1} = \frac{a'_1}{b'_1}$ et $\frac{a_2}{b_2} = \frac{a'_2}{b'_2}$. Alors

$$(a_1 b_2 + a_2 b_1) b'_1 b'_2 = a_1 b'_1 b_2 b'_2 + a_2 b'_2 b_1 b'_1 = a'_1 b_1 b_2 b'_2 + a'_2 b_2 b_1 b'_1 = (a'_1 b'_2 + a'_2 b'_1) b_1 b_2,$$

donc

$$\frac{a_1 b_2 + a_2 b_1}{b_1 b_2} = \frac{a'_1 b'_2 + a'_2 b'_1}{b'_1 b'_2}.$$

De plus

$$a_1 a_2 b'_1 b'_2 = a'_1 a'_2 b_1 b_2,$$

donc

$$\frac{a_1 a_2}{b_1 b_2} = \frac{a'_1 a'_2}{b'_1 b'_2}.$$

Montrons que \mathbb{K} muni de ces deux opérations est un corps. On pose $0_{\mathbb{K}} = \frac{0}{1}$ et $1_{\mathbb{K}} = \frac{1}{1}$.

$$\begin{aligned} \left(\frac{a_1}{b_1} + \frac{a_2}{b_2}\right) + \frac{a_3}{b_3} &= \frac{a_1 b_2 b_3 + a_2 b_1 b_3 + a_3 b_1 b_2}{b_1 b_2 b_3} = \frac{a_1}{b_1} + \left(\frac{a_2}{b_2} + \frac{a_3}{b_3}\right), \\ \frac{a_1}{b_1} + \frac{a_2}{b_2} &= \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} = \frac{a_2}{b_2} + \frac{a_1}{b_1}, \\ \frac{a_1}{b_1} + 0_{\mathbb{K}} &= \frac{a_1 \cdot 1 + 0 \cdot b_1}{b_1 \cdot 1} = \frac{a_1}{b_1}, \\ \frac{a_1}{b_1} + \frac{-a_1}{b_1} &= \frac{a_1 b_1 - a_1 b_1}{b_1^2} = \frac{0}{b_1^2} = \frac{0}{1} = 0_{\mathbb{K}}, \end{aligned}$$

donc $(\mathbb{K}, +)$ est un groupe abélien. De plus,

$$\begin{aligned} \left(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2}\right) \cdot \frac{a_3}{b_3} &= \frac{a_1 a_2 a_3}{b_1 b_2 b_3} = \frac{a_1}{b_1} \cdot \left(\frac{a_2}{b_2} \cdot \frac{a_3}{b_3}\right), \\ \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} &= \frac{a_1 a_2}{b_1 b_2} = \frac{a_2}{b_2} \cdot \frac{a_1}{b_1}, \\ \frac{a_1}{b_1} \cdot 1_{\mathbb{K}} &= \frac{a_1 \cdot 1}{b_1 \cdot 1} = \frac{a_1}{b_1}, \\ \frac{a_1}{b_1} \cdot \frac{b_1}{a_1} &= \frac{a_1 b_1}{a_1 b_1} = \frac{1}{1} = 1_{\mathbb{K}}, \text{ si } a_1 \neq 0. \end{aligned}$$

Finalement,

$$\frac{a_1}{b_1} \left(\frac{a_2}{b_2} + \frac{a_3}{b_3}\right) = \frac{a_1 a_2 b_3 + a_1 a_3 b_2}{b_1 b_2 b_3} = \frac{a_1 a_2 b_1 b_3 + a_1 a_3 b_1 b_2}{b_1^2 b_2 b_3} = \left(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2}\right) + \left(\frac{a_1}{b_1} \cdot \frac{a_3}{b_3}\right).$$

Montrons que l'application

$$\begin{aligned} \varphi : A &\rightarrow \mathbb{K} \\ a &\mapsto \frac{a}{1} \end{aligned}$$

est un homomorphisme injectif.

$$\begin{aligned} \varphi(a) + \varphi(b) &= \frac{a}{1} + \frac{b}{1} = \frac{a \cdot 1 + b \cdot 1}{1} = \frac{a + b}{1} = \varphi(a + b), \\ \varphi(a) \cdot \varphi(b) &= \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1} = \varphi(ab), \\ \varphi(1) &= \frac{1}{1} = 1_{\mathbb{K}}, \end{aligned}$$

donc φ est un homomorphisme. Soit $a \in \text{Ker } \varphi$. Alors $\frac{a}{1} = \frac{0}{1}$, donc $a = 0$. Ceci montre que φ est injectif.

Soit $x \in \mathbb{K}$. Il existe $(a, b) \in A \times A \setminus \{0\}$ tel que $x = \frac{a}{b}$. Alors

$$bx = \frac{ab}{b} = \frac{a}{1} = a \in A.$$

Soit \mathbb{F} un corps tel que A soit un sous-anneau de \mathbb{F} et, pour tout $x \in \mathbb{F}$, il existe $a \in A$ tel que $ax \in A$. Soit $\tilde{f} : A \times A \setminus \{0\} \rightarrow \mathbb{F}$ l'application définie par

$$\tilde{f}(a, b) = ab^{-1}.$$

On vérifie facilement que, si $(a, b) \sim (a', b')$, alors $\tilde{f}(a, b) = \tilde{f}(a', b')$. Ceci implique que \tilde{f} induit une application $f : \mathbb{K} \rightarrow \mathbb{F}$. Celle-ci est définie par

$$f\left(\frac{a}{b}\right) = ab^{-1}.$$

On vérifie facilement que $f : \mathbb{K} \rightarrow \mathbb{F}$ est un homomorphisme. Il est injectif par le lemme 1.25. Montrons qu'il est surjectif. Soit $x \in \mathbb{F}$. Il existe $b \in A$, $b \neq 0$, tel que $bx = a \in A$. Alors $x = f\left(\frac{a}{b}\right)$. \square

Définition. Le corps \mathbb{K} du théorème 2.2 s'appelle le *corps des fractions* de A .

Exemple. Soit \mathbb{K} un corps. Alors le corps des fractions de $\mathbb{K}[X]$ se note $\mathbb{K}(X)$ et s'appelle le *corps des fractions rationnelles* à coefficients dans \mathbb{K} .

Lemme 2.3. Soient A un anneau factoriel et $a_1, \dots, a_n \in A$ des éléments non tous nuls. Alors il existe $c \in A$ tel que

- (a) c divise a_i pour tout $i \in \{1, \dots, n\}$;
- (b) si $c' \in A$ divise a_i pour tout $i \in \{1, \dots, n\}$, alors c' divise c .

Démonstration. Exercice. \square

Définition. L'élément c du lemme 2.3 s'appelle un pgcd de a_1, \dots, a_n . On vérifie facilement que, si c, c' sont deux pgcd de a_1, \dots, a_n , alors il existe $u \in U(A)$ tel que $c' = uc$.

Définition. Soient A un anneau factoriel, \mathbb{K} son corps de fractions et $f \in \mathbb{K}[X]$ un polynôme non nul. On écrit

$$f = \alpha_0 + \alpha_1 X + \dots + \alpha_n X^n.$$

On choisit $a_0, a_1, \dots, a_n, b \in A$ tels que $\alpha_i = \frac{a_i}{b}$ pour tout $i \in \{0, 1, \dots, n\}$. Soit c un pgcd de a_0, a_1, \dots, a_n . Alors $\gamma = \frac{c}{b}$ s'appelle un *contenu* de f .

Lemme 2.4. *La définition de contenu donnée ci-dessus ne dépend pas du choix de a_0, a_1, \dots, a_n, b .*

Démonstration. soient $a'_0, a'_1, \dots, a'_n, b' \in A$ tels que $\alpha_i = \frac{a'_i}{b'}$ pour tout $i \in \{0, 1, \dots, n\}$. Soit c' un pgcd de a'_0, a'_1, \dots, a'_n . Comme $c'b$ est un pgcd de $a'_0b, a'_1b, \dots, a'_nb$, cb' est un pgcd de $a_0b', a_1b', \dots, a_nb'$ et $a'_ib = a_ib'$ pour tout $i \in \{0, 1, \dots, n\}$, il existe $u \in U(A)$ tel que $c'b = ucb'$. Il en résulte que $\frac{c'}{b'} = \frac{uc}{b}$. \square

Définition. Soient A un anneau factoriel et \mathbb{K} le corps des fractions de A . Si $f \in \mathbb{K}[X]$ est un polynôme non nul, on note $\mathcal{C}(f)$ l'ensemble des contenus de f . Il est clair que si $\gamma, \gamma' \in \mathcal{C}(f)$, alors il existe $u \in U(A)$ tel que $\gamma' = u\gamma$. On dit que $f \in \mathbb{K}[X]$ est *primitif* si 1 est un contenu de f ou, de façon équivalente, si $\mathcal{C}(f) = U(A)$.

Proposition 2.5. *Soient A un anneau factoriel et \mathbb{K} le corps des fractions de A .*

- (1) *Soient $f \in \mathbb{K}[X]$ un polynôme non nul, γ un contenu de f et $\alpha \in \mathbb{K} \setminus \{0\}$. Alors $\alpha\gamma$ est un contenu de f . En particulier, $\frac{1}{\gamma}f$ est un polynôme primitif.*
- (2) *Si $f \in \mathbb{K}[X]$ est un polynôme primitif, alors $f \in A[X]$.*

Démonstration. Soient $f \in \mathbb{K}[X]$ un polynôme non nul, γ un contenu de f et $\alpha \in \mathbb{K} \setminus \{0\}$. Posons

$$f = \alpha_0 + \alpha_1X + \dots + \alpha_nX^n.$$

On choisit $a_0, a_1, \dots, a_n, b \in A$ tels que $\alpha_i = \frac{a_i}{b}$ pour tout $i \in \{0, 1, \dots, n\}$. Alors, par définition, il existe un pgcd c de a_0, a_1, \dots, a_n tel que $\gamma = \frac{c}{b}$. Par ailleurs, on choisit $a', b' \in A$ tels que $\alpha = \frac{a'}{b'}$. Alors

$$\alpha f = (\alpha\alpha_0) + (\alpha\alpha_1)X + \dots + (\alpha\alpha_n)X^n,$$

$\alpha\alpha_i = \frac{a'a_i}{b'b}$ pour tout $i \in \{0, 1, \dots, n\}$, et $a'c$ est un pgcd de $a'a_0, a'a_1, \dots, a'a_n$, donc $\alpha\gamma = \frac{a'c}{b'b}$ est un contenu de αf .

Soit $f \in \mathbb{K}[X]$ un polynôme non nul primitif. Posons

$$f = \alpha_0 + \alpha_1X + \dots + \alpha_nX^n.$$

On choisit $a_0, a_1, \dots, a_n, b \in A$ tels que $\alpha_i = \frac{a_i}{b}$ pour tout $i \in \{0, 1, \dots, n\}$. Comme f est primitif, il existe un pgcd c de a_0, a_1, \dots, a_n tel que $1 = \frac{c}{b}$. En particulier, $b = c$ divise a_i pour tout $i \in \{0, 1, \dots, n\}$. On note a'_i l'élément de A vérifiant $a_i = a'_ib$. On a $\alpha_i = \frac{a'_i}{b} \in A$ pour tout $i \in \{0, 1, \dots, n\}$, donc $f \in A[X]$. \square

Théorème 2.6 (Lemme de Gauss). *Soient A un anneau factoriel et \mathbb{K} son corps de fractions. Soient $f, g \in \mathbb{K}[X]$ deux polynômes non nuls, γ un contenu de f et δ un contenu de g . Alors $\gamma\delta$ est un contenu de fg .*

Démonstration. Supposons d'abord que f et g sont primitifs. En particulier, par la proposition 2.5, $f, g \in A[X]$. Posons

$$f = a_0 + a_1X + \cdots + a_nX^n, \quad g = b_0 + b_1X + \cdots + b_mX^m.$$

Soit p un élément premier de A . Comme f est primitif, les a_i sont premiers entre eux et donc p ne peut pas diviser tous les a_i . De même, p ne peut pas diviser tous les b_j . Posons

$$r = \min\{i \in \{0, 1, \dots, n\} ; p \text{ ne divise pas } a_i\}, \\ s = \min\{j \in \{0, 1, \dots, m\} ; p \text{ ne divise pas } b_j\}.$$

Par ce qui précède, r et s existent. Le $(r+s)$ -ème coefficient de fg est

$$c_{r+s} = a_r b_s + \sum_{i=0}^{r-1} a_i b_{r+s-i} + \sum_{j=0}^{s-1} a_{s+r-j} b_j.$$

p divise $a_i b_{r+s-i}$ pour tout $i \in \{0, \dots, r-1\}$, p divise $a_{s+r-j} b_j$ pour tout $j \in \{0, \dots, s-1\}$ et p ne divise pas $a_r b_s$, donc

$$c_{r+s} \equiv a_r b_s \pmod{p} \not\equiv 0 \pmod{p},$$

donc p ne divise pas c_{r+s} . Donc, aucun élément premier divise tous les coefficients de fg , donc les coefficients de fg sont premiers entre eux, donc fg est primitif.

Supposons maintenant que f, g sont quelconques et, comme dans l'énoncé, γ est un contenu de f et δ est un contenu de g . Par la proposition 2.5 $\frac{1}{\gamma}f$ et $\frac{1}{\delta}g$ sont des polynômes primitifs. Par ce qui précède, il s'en suit que $(\frac{1}{\gamma}f)(\frac{1}{\delta}g) = \frac{1}{\gamma\delta}fg$ est primitif, donc 1 est un contenu de $\frac{1}{\gamma\delta}fg$. Par la proposition 2.5 on en conclue que $\gamma\delta$ est un contenu de $\gamma\delta\frac{1}{\gamma\delta}fg = fg$. \square

Théorème 2.7. Soient A un anneau factoriel et \mathbb{K} le corps des fractions de A .

- (1) $A[X]$ est factoriel.
- (2) Soit $P \in A[X]$ un polynôme non nul. Alors P est premier dans $A[X]$ si et seulement si :
 - (i) $P = p$ est un élément premier de A ; ou bien
 - (ii) P est primitif et est premier dans $\mathbb{K}[X]$.

Démonstration. Rappelons que $U(A[X]) = U(A)$ (voir Lemme 1.8). Soit $f \in A[X]$, $f \notin U(A)$. Pour démontrer le théorème il suffit de montrer

(1) f s'écrit sous la forme

$$f = c_1 \cdots c_l P_1 \cdots P_r,$$

où c_1, \dots, c_l sont des éléments premiers de A et P_1, \dots, P_r sont des polynôme primitifs et premiers dans $\mathbb{K}[X]$.

(2) Si

$$f = c_1 \cdots c_l P_1 \cdots P_r = d_1 \cdots d_k Q_1 \cdots Q_s,$$

où $c_1, \dots, c_l, d_1, \dots, d_k$ sont des éléments premiers de A et $P_1, \dots, P_r, Q_1, \dots, Q_s$ sont des polynômes primitifs premiers dans $\mathbb{K}[X]$, alors $l = k, r = s$ et, à permutation près, il existe des unités $u_1, \dots, u_l, v_1, \dots, v_r \in U(A)$ telles que $d_i = u_i c_i$ pour tout $i \in \{1, \dots, l\}$ et $Q_j = v_j P_j$ pour tout $j \in \{1, \dots, r\}$.

Comme $\mathbb{K}[X]$ est factoriel (voir corollaire 1.7), il existe des polynômes premiers P'_1, \dots, P'_r dans $\mathbb{K}[X]$ tels que

$$f = P'_1 \cdots P'_r.$$

Pour tout $i \in \{1, \dots, r\}$ on se donne un contenu a_i de P'_i et on pose $P_i = \frac{1}{a_i} P'_i$. Par la Proposition 2.5 P_i est primitif. Il est premier dans $\mathbb{K}[X]$ car P'_i l'est. Par ailleurs, on pose $a = a_1 \cdots a_r$. On a

$$f = a P_1 \cdots P_r.$$

Comme 1 est un contenu de P_i pour tout $i \in \{1, \dots, r\}$, par la proposition 2.5 et le théorème 2.6 a est un contenu de f . Comme $f \in A[X]$, on a en particulier $a \in A$. Comme A est factoriel, a s'écrit sous la forme $a = c_1 \cdots c_l$ où c_1, \dots, c_l sont des éléments premiers de A . Finalement,

$$f = c_1 \cdots c_l P_1 \cdots P_r.$$

Maintenant on suppose que f s'écrit

$$f = c_1 \cdots c_l P_1 \cdots P_r = d_1 \cdots d_k Q_1 \cdots Q_s,$$

où $c_1, \dots, c_l, d_1, \dots, d_k$ sont des éléments premiers de A et $P_1, \dots, P_r, Q_1, \dots, Q_s$ sont des polynômes primitifs premiers dans $\mathbb{K}[X]$. Par la proposition 2.5 et le théorème 2.6, $c_1 \cdots c_l$ et $d_1 \cdots d_k$ sont des contenus de f , donc il existe $w \in U(A)$ tel que $d_1 \cdots d_k = w c_1 \cdots c_l$. Comme A est factoriel, il s'en suit que $k = l$ et il existe de unités $u_1, \dots, u_l \in U(A)$ tels que $d_i = u_i c_i$, à permutation près. Par ailleurs, comme $\mathbb{K}[X]$ est factoriel, on a $r = s$ et il existe $v_1, \dots, v_r \in \mathbb{K}^*$ tels que $Q_j = v_j P_j$ à permutation près. Par la proposition 2.5, v_j est un contenu de Q_j , qui est primitif, donc $v_j \in U(A)$. \square

Corollaire 2.8. *Soit A un anneau factoriel et $n \geq 1$. Alors l'anneau $A[X_1, \dots, X_n]$ des polynômes à n variables à coefficients dans A est factoriel.*

Démonstration. Raisonner par récurrence sur n . \square

Remarque. Si \mathbb{K} est un corps et $n \geq 2$, alors $\mathbb{K}[X_1, \dots, X_n]$ n'est pas principal. Par exemple, l'idéal engendré par X_1, \dots, X_n n'est pas monogène (exercice).

3 Critères d'irréductibilité

Théorème 3.1 (Critère d'Eisenstein). Soient A un anneau factoriel, \mathbb{K} le corps des fractions de A et $f = a_0 + a_1X + \dots + a_nX^n$ un polynôme dans $A[X]$ de degré $n \geq 1$. S'il existe un élément premier p de A tel que

$$\begin{aligned} a_n &\not\equiv 0 \pmod{p} \\ a_i &\equiv 0 \pmod{p} \quad \text{pour tout } i \in \{0, \dots, n-1\} \\ a_0 &\not\equiv 0 \pmod{p^2} \end{aligned}$$

alors f est premier dans $\mathbb{K}[X]$.

Démonstration. Soit c un contenu de f et $\tilde{f} = \frac{1}{c}f = \tilde{a}_0 + \tilde{a}_1X + \dots + \tilde{a}_nX^n$. On a $a_i = c\tilde{a}_i$ pour tout $i \in \{0, 1, \dots, n\}$. Comme p ne divise pas a_n , p ne divise ni c , ni \tilde{a}_n . Pour $i \in \{0, 1, \dots, n-1\}$, p divise $a_i = c\tilde{a}_i$ et p ne divise pas c , donc p divise \tilde{a}_i . Comme p^2 ne divise pas $a_0 = c\tilde{a}_0$, p^2 ne divise pas \tilde{a}_0 . Finalement, f est premier si et seulement si \tilde{f} l'est. Donc, quitte à remplacer f par \tilde{f} , on peut supposer que f est primitif.

On raisonne par l'absurde en supposant que f n'est pas irréductible. Il existe donc des polynômes $\tilde{g}, \tilde{h} \in \mathbb{K}[X]$ tels que $\deg \tilde{g}, \deg \tilde{h} \geq 1$ et $f = \tilde{g}\tilde{h}$. Soient c un contenu de \tilde{g} et d un contenu de \tilde{h} . Posons

$$g = \frac{1}{c}\tilde{g}, \quad h = \frac{1}{d}\tilde{h}.$$

Comme f est primitif et, par le théorème 2.6, cd est un contenu de f , on a $cd = u \in U(A)$. Quitte à remplacer f par $u^{-1}f$, on peut supposer que $f = gh$. Remarquez que g, h sont primitifs et donc sont dans $A[X]$.

Posons

$$g = b_0 + b_1X + \dots + b_dX^d, \quad h = c_0 + c_1X + \dots + c_mX^m$$

avec $b_d \neq 0$ et $c_m \neq 0$. $a_0 = b_0c_0$ est divisible par p mais pas par p^2 , donc p divise b_0 ou c_0 mais pas les deux à la fois. On peut en toute généralité supposer que p divise c_0 mais pas b_0 . Soit

$$r = \min\{i; p \text{ ne divise pas } c_i\}.$$

Comme p ne divise pas $a_n = b_dc_m$, p ne divise pas c_m . Par ailleurs, p divise c_0 , donc r existe et $1 \leq r \leq m < n$. On a

$$a_r = b_0c_r + \sum_{i=0}^{r-1} b_{r-i}c_i.$$

On observe que p divise a_r et p divise $b_{r-i}c_i$ pour tout $i \in \{0, \dots, r-1\}$, donc p doit diviser b_0c_r . Or p ne divise ni b_0 ni c_r : contradiction. \square

Exemples.

- (1) $3X^5 - 15$ et $2X^{10} - 21$ sont premiers dans $\mathbb{Q}[X]$.

(2) Soient $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ sans facteur carré, et $n \in \mathbb{N}$, $n \geq 1$. alors $X^n - a$ est irréductible dans $\mathbb{Q}[X]$.

(3) Si p est un nombre premier, alors

$$1 + X + \dots + X^{p-1}$$

est irréductible dans $\mathbb{Q}[X]$.

(4) Soient \mathbb{K} un corps et $\mathbb{K}(X)$ le corps des fractions rationnelles sur \mathbb{K} . Alors, pour $n \in \mathbb{N}$, $n \geq 1$, le polynôme $Y^n - X \in \mathbb{K}(X)[Y]$ est premier.

Démonstration. Exercice. □

Définition. Soient A, B deux anneaux et $\varphi : A \rightarrow B$ un homomorphisme. Soit $\tilde{\varphi} : A[X] \rightarrow B[X]$ l'application définie par

$$\tilde{\varphi}(a_0 + a_1X + \dots + a_nX^n) = \varphi(a_0) + \varphi(a_1)X + \dots + \varphi(a_n)X^n.$$

On vérifie facilement que $\tilde{\varphi}$ est un homomorphisme. Il s'appelle l'homomorphisme *induit* par φ .

Proposition 3.2. Soient A, B deux anneaux intègres, \mathbb{K}, \mathbb{L} les corps de fractions de A et B , respectivement, $\varphi : A \rightarrow B$ un homomorphisme, et $\tilde{\varphi} : A[X] \rightarrow B[X]$ l'homomorphisme induit par φ . Soit $f \in A[X]$ un polynôme de degré ≥ 1 . Si $\tilde{\varphi}(f)$ est irréductible dans $\mathbb{L}[X]$ et $\deg \varphi(f) = \deg f$, alors f ne se décompose pas sous la forme $f = gh$ avec $g, h \in A[X]$, $\deg g \geq 1$ et $\deg h \geq 1$.

Démonstration. On raisonne par l'absurde en supposant qu'il existe deux polynômes $g, h \in A[X]$ tels que $\deg g \geq 1$, $\deg h \geq 1$ et $f = gh$. En particulier, comme $\deg f = \deg g + \deg h$, on a $\deg g < \deg f$ et $\deg h < \deg f$. En appliquant $\tilde{\varphi}$ on obtient $\tilde{\varphi}(f) = \tilde{\varphi}(g)\tilde{\varphi}(h)$ et

$$\deg \tilde{\varphi}(g) \leq \deg g < \deg f, \quad \deg \tilde{\varphi}(h) \leq \deg h < \deg f.$$

Par ailleurs, comme $\tilde{\varphi}(f)$ est irréductible, on doit avoir $\deg \tilde{\varphi}(g) = \deg \tilde{\varphi}(f) = \deg f$ ou $\deg \tilde{\varphi}(h) = \deg \tilde{\varphi}(f) = \deg f$: contradiction. □

Corollaire 3.3. Soient A un anneau factoriel, \mathbb{K} le corps de fractions de A , \mathbb{L} un autre corps, $\varphi : A \rightarrow \mathbb{L}$ un homomorphisme, et $\tilde{\varphi} : A[X] \rightarrow \mathbb{L}[X]$ l'homomorphisme induit par φ . Soit $f \in A[X]$ un polynôme de degré ≥ 1 . Si $\tilde{\varphi}(f)$ est irréductible dans $\mathbb{L}[X]$ et $\deg \varphi(f) = \deg f$, alors f est irréductible dans $\mathbb{K}[X]$.

Démonstration. On raisonne par l'absurde et on suppose que f n'est pas irréductible dans $\mathbb{K}[X]$. Soit a un contenu f et posons $\tilde{f} = \frac{1}{a}f$. Alors \tilde{f} est primitif et est réductible dans $\mathbb{K}[X]$. Soient $\tilde{g}, \tilde{h} \in \mathbb{K}[X]$ de degré ≥ 1 tels que $\tilde{f} = \tilde{g}\tilde{h}$. Soient b, c des contenus de \tilde{g}, \tilde{h} , respectivement, $g = \frac{1}{b}\tilde{g}$, et $h = \frac{1}{c}\tilde{h}$. On observe que bc est un contenu de f qui est

primitif, donc on peut supposer que $bc = 1$, donc $\tilde{f} = gh$, donc $f = (ag)h$. Ceci contredit la proposition 3.2 car $ag, h \in A[X]$. \square

Exemple.

$$X^5 - 5X^4 + 6X - 1$$

est irréductible dans $\mathbb{Q}[X]$.

Proposition 3.4 (Test de la racine). *Soient A un anneau factoriel et \mathbb{K} le corps des fractions de A . Soit*

$$f = a_0 + a_1X + \cdots + a_nX^n, \quad a_n \neq 0,$$

un polynôme à coefficients dans A . Soit $\alpha = \frac{b}{c}$ une racine de f dans \mathbb{K} , où b, c sont deux éléments de A premiers entre eux. Alors b divise a_0 et c divise a_n . En particulier, si $a_n = 1$, on doit avoir $\alpha \in A$ et α divise a_0 .

Démonstration. Exercice. \square

4 Théorème de la base de Hilbert

Proposition 4.1. *Les conditions suivantes sur un anneau A sont équivalentes :*

(a) *Tout idéal de A est de génération finie (i.e. si $I \subset A$ est un idéal, alors il existe un nombre fini d'éléments $a_1, \dots, a_n \in I$ tels que $I = (a_1, \dots, a_n)$).*

(b) *Toute chaîne croissante*

$$I_1 \subset \cdots \subset I_k \subset I_{k+1} \subset \cdots$$

d'idéaux est stationnaire (i.e. il existe $N \in \mathbb{N}$ tel que $I_k = I_N$ pour tout $k \geq N$).

(c) *Tout ensemble non vide d'idéaux de A a au moins un élément maximal (pour l'inclusion).*

Définition. Un anneau A vérifiant les conditions de la proposition 4.1 est dit *noethérien*.

Démonstration. (a) \Rightarrow (b) : Soit

$$I_1 \subset I_2 \subset \cdots \subset I_k \subset \cdots$$

un chaîne croissante d'idéaux. Posons

$$I = \bigcup_{k=1}^{\infty} I_k.$$

On vérifie facilement que I est un idéal de A . Par (a), I est de génération finie, c'est-à-dire qu'il existe un nombre fini d'éléments $a_1, \dots, a_n \in I$ tels que $I = (a_1, \dots, a_n)$. Pour

tout $i \in \{1, \dots, n\}$ il existe $N_i \in \mathbb{N}$ tel que $a_i \in I_{N_i}$. Soit $N = \max\{N_1, \dots, N_n\}$. Alors $a_i \in I_N \subset I_N$ pour tout $i \in \{1, \dots, n\}$, donc $I \subset I_N$. Si $k \geq N$, alors

$$I_N \subset I_k \subset I \subset I_N,$$

donc $I_N = I_k$.

(b) \Rightarrow (c) : On raisonne par l'absurde. On suppose qu'il existe un ensemble non vide \mathcal{E} d'idéaux de A n'ayant pas d'élément maximal pour l'inclusion. On construit une chaîne d'idéaux $\{I_k\}_{k=1}^\infty$ comme suit. I_1 est un élément choisi quelconque de \mathcal{E} . Pour tout $n \in \mathbb{N}$, I_{n+1} est un idéal dans \mathcal{E} tel que $I_n \subsetneq I_{n+1}$. La suite ainsi construite est une chaîne croissante d'idéaux non stationnaire. Ceci contredit (b).

(c) \Rightarrow (a) : Soit I un idéal de A . Notons \mathcal{E} l'ensemble des idéaux de génération finie inclus dans I . On a $\mathcal{E} \neq \emptyset$ car $(0) = \{0\} \in \mathcal{E}$. Par (c), \mathcal{E} possède un élément maximal, J . Montrons que $J = I$ par l'absurde. Supposons que $J \neq I$. Comme $J \subset I$, cela signifie que $I \setminus J \neq \emptyset$. Choisissons $b \in I \setminus J$ et posons $J' = (a_1, \dots, a_n, b)$, où a_1, \dots, a_n sont tels que $J = (a_1, \dots, a_n)$. Comme $a_1, \dots, a_n, b \in I$, on a $J' \subset I$, donc $J' \in \mathcal{E}$. Comme $a_1, \dots, a_n \in J'$, on a $J \subset J'$. Finalement, $b \in J'$ mais $b \notin J$, donc $J \neq J'$. Ceci contredit la maximalité de J . \square

Proposition 4.2.

- (1) Soient A un anneau noethérien et $I \subset A$ un idéal propre. Alors A/I est noethérien.
- (2) Soient A un anneau noethérien, \mathbb{K} le corps des fractions de A , et $S \subset A$ une partie non vide ne contenant pas 0. Soit B l'ensemble des éléments de \mathbb{K} de la forme $\frac{a}{b}$ avec $a \in A$ et b un produit d'éléments de S . Alors B est un sous-anneau de \mathbb{K} , et B est noethérien.

Démonstration. Exercice. \square

Théorème 4.3 (Théorème de la base de Hilbert). *Si A est un anneau noethérien, alors $A[X]$ est aussi noethérien.*

Démonstration. Soit J un idéal non nul de $A[X]$. Pour tout $n \in \mathbb{N}$ on pose

$$I_n = \{a \in A ; \text{il existe } f \in J \text{ tel que } \deg f = n \text{ et } \text{cd}(f) = a\} \cup \{0\}.$$

Montrons que I_n est un idéal de A . Soient $a_1, a_2 \in I_n \setminus \{0\}$ et $b_1, b_2 \in A$. Soient $f_1, f_2 \in J$ tels que $\deg f_1 = \deg f_2 = n$ et $\text{cd}(f_1) = a_1$ et $\text{cd}(f_2) = a_2$. On a $b_1 a_1 + b_2 a_2 = 0$, ou bien $b_1 f_1 + b_2 f_2 \in J$, $\deg(b_1 f_1 + b_2 f_2) = n$ et $\text{cd}(b_1 f_1 + b_2 f_2) = b_1 a_1 + b_2 a_2$. Dans les deux cas on a $b_1 a_1 + b_2 a_2 \in I_n$. On montre encore plus facilement que $b_1 a_1 + b_2 a_2 \in I_n$ si $a_1 = 0$ ou $a_2 = 0$ et $a_1, a_2 \in I_n$.

On montre que $I_n \subset I_{n+1}$ pour tout $n \in \mathbb{N}$. Soit $a \in I_n \setminus \{0\}$. Soit $f \in J$ tel que $\deg(f) = n$ et $\text{cd}(f) = a$. Alors $fX \in J$, $\deg(fX) = n+1$ et $\text{cd}(fX) = a$, donc $a \in I_{n+1}$.

Comme A est noethérien, il existe $N \in \mathbb{N}$ tel que $I_k = I_N$ pour $k \geq N$. Pour tout $k \in \{0, 1, \dots, N\}$ on choisit une famille finie $\{a_{k,1}, \dots, a_{k,l_k}\}$ qui engendre I_k . Pour tous $k \in \{0, 1, \dots, N\}$ et $i \in \{1, \dots, l_k\}$ on choisit $f_{k,i} \in J$ tel que $\deg f_{k,i} = k$ et $\text{cd}(f_{k,i}) = a_{k,i}$. On pose

$$J' = (f_{k,i} \mid 0 \leq k \leq N \text{ et } 1 \leq i \leq l_k).$$

On va montrer que $J' = J$.

Comme $f_{k,i} \in J$ pour tout k, i on a $J' \subset J$. Reste à montrer que $J \subset J'$. On se donne $f \in J$ et on montre par récurrence sur $n = \deg f$ que $f \in J'$. Si $n = -\infty$, c'est-à-dire $f = 0$, alors $f \in J'$ par définition. On peut donc supposer que $n \geq 0$.

Supposons que $n = 0$. Alors $\deg f = 0$, donc $f = c$ est constant. On a $c \in I_0$ donc il existe $b_1, \dots, b_{l_0} \in A$ tels que

$$f = c = b_1 a_{0,1} + \dots + b_{l_0} a_{0,l_0} = b_1 f_{0,1} + \dots + b_{l_0} f_{0,l_0}.$$

D'où $f \in J'$.

Supposons que $n \geq 1$ plus l'hypothèse de récurrence. Posons $c = \text{cd}(f)$. On a $c \in I_n$. Supposons d'abord que $n \leq N$. Il existe $b_1, \dots, b_{l_n} \in A$ tels que

$$c = b_1 a_{n,1} + \dots + b_{l_n} a_{n,l_n}.$$

Posons

$$f' = f - b_1 f_{n,1} - \dots - b_{l_n} f_{n,l_n}.$$

On observe que $f' \in J$ et $\deg f' < \deg f = n$. Par hypothèse de récurrence, on a $f' \in J'$, d'où

$$f = f' + b_1 f_{n,1} + \dots + b_{l_n} f_{n,l_n} \in J'.$$

Supposons que $n > N$. Il existe $b_1, \dots, b_{l_N} \in A$ tels que

$$c = b_1 a_{N,1} + \dots + b_{l_N} a_{N,l_N}.$$

Posons

$$f' = f - b_1 f_{N,1} X^{n-N} - \dots - b_{l_N} f_{N,l_N} X^{n-N}.$$

On observe que $f' \in J$ et $\deg f' < \deg f = n$. Par hypothèse de récurrence, on a $f' \in J'$, d'où

$$f = f' + b_1 f_{N,1} X^{n-N} + \dots + b_{l_N} f_{N,l_N} X^{n-N} \in J'.$$

□

5 Polynômes symétriques

Définition. Soient A un anneau (commutatif), t_1, \dots, t_n des indéterminées sur A (algébriquement indépendantes), et X une indéterminée sur $A[t_1, \dots, t_n]$. On considère le polynôme

$$F = (X - t_1)(X - t_2) \cdots (X - t_n) \in A[t_1, \dots, t_n][X]$$

que l'on développe :

$$F = X^n - s_1 X^{n-1} + \cdots + (-1)^{n-1} s_{n-1} X + (-1)^n s_n,$$

où $s_1, \dots, s_n \in A[t_1, \dots, t_n]$. Les polynômes $s_1, \dots, s_n \in A[t_1, \dots, t_n]$ s'appellent les *polynômes symétriques élémentaires*.

Exemple. Supposons que $n = 2$. Alors

$$(X - t_1)(X - t_2) = X^2 - (t_1 + t_2)X + t_1 t_2,$$

donc

$$s_1 = t_1 + t_2, \quad s_2 = t_1 t_2.$$

Supposons que $n = 3$. Alors

$$(X - t_1)(X - t_2)(X - t_3) = X^3 - (t_1 + t_2 + t_3)X^2 + (t_1 t_2 + t_1 t_3 + t_2 t_3)X - t_1 t_2 t_3,$$

donc

$$s_1 = t_1 + t_2 + t_3, \quad s_2 = t_1 t_2 + t_1 t_3 + t_2 t_3, \quad s_3 = t_1 t_2 t_3.$$

Plus généralement, on a :

Lemme 5.1. Soit $n \geq 2$ fixé. Alors, pour tout $k \in \{1, \dots, n\}$,

$$s_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} t_{i_1} \cdots t_{i_k}.$$

En particulier, s_k est un polynôme homogène de degré k .

Démonstration. On raisonne par récurrence sur n . Le cas $n = 2$ étant traité dans l'exemple précédent, on peut supposer que $n \geq 3$ plus l'hypothèse de récurrence. Notons s'_1, \dots, s'_{n-1} les polynômes symétriques élémentaires en t_1, \dots, t_{n-1} . Par ailleurs, pour simplifier les notations, on posera $s_0 = s'_0 = 1$. On a

$$\begin{aligned} \prod_{k=1}^n (X - t_k) &= \left(\sum_{k=0}^{n-1} (-1)^k s'_k X^{n-1-k} \right) (X - t_n) \\ &= X^n + \sum_{k=1}^{n-1} (-1)^k (s'_k + s'_{k-1} t_n) X^{n-k} + (-1)^n s'_{n-1} t_n, \end{aligned}$$

donc

$$\begin{aligned} s_n &= s'_{n-1}t_n \\ s_k &= s'_k + s'_{k-1}t_n \quad \text{pour } 1 \leq k \leq n-1. \end{aligned}$$

En appliquant la récurrence à cette égalité on obtient

$$s_n = (t_1 \cdots t_{n-1})t_n = t_1 \cdots t_{n-1}t_n$$

et

$$s_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n-1} t_{i_1} \cdots t_{i_k} + \sum_{1 \leq i_1 < \cdots < i_{k-1} \leq n-1} t_{i_1} \cdots t_{i_{k-1}}t_n = \sum_{1 \leq i_1 < \cdots < i_k \leq n} t_{i_1} \cdots t_{i_k}.$$

pour tout $k \in \{1, \dots, n-1\}$. □

Définition. Soient A un anneau commutatif et t_1, \dots, t_n des indéterminées sur A . Pour toute permutation $w \in \mathfrak{S}_n$ et tout $f \in A[t_1, \dots, t_n]$ on pose

$$(w \cdot f)(t_1, \dots, t_n) = f(t_{w(1)}, \dots, t_{w(n)}) \in A[t_1, \dots, t_n].$$

Lemme 5.2.

(1) Pour tout $w \in \mathfrak{S}_n$ l'application

$$\begin{array}{ccc} \rho(w) : A[t_1, \dots, t_n] & \rightarrow & A[t_1, \dots, t_n] \\ f & \mapsto & w \cdot f \end{array}$$

est un automorphisme.

(2) L'application

$$\begin{array}{ccc} \rho : \mathfrak{S}_n & \rightarrow & \text{Aut}(A[t_1, \dots, t_n]) \\ w & \mapsto & \rho(w) \end{array}$$

est un homomorphisme de groupes.

Démonstration. La partie (1) est facile à démontrer et est laissée en exercice. Démontrons la partie (2). Soient $v, w \in \mathfrak{S}_n$. Pour tout $f \in A[t_1, \dots, t_n]$ on a

$$\begin{aligned} v \cdot (w \cdot f)(t_1, \dots, t_n) &= (w \cdot f)(t_{v(1)}, \dots, t_{v(n)}) \\ &= f(t_{vw(1)}, \dots, t_{vw(n)}) \\ &= (vw \cdot f)(t_1, \dots, t_n) \end{aligned}$$

donc $\rho(v) \circ \rho(w) = \rho(vw)$. □

Définition. Un polynôme $f \in A[t_1, \dots, t_n]$ est dit *symétrique* si $w \cdot f = f$ pour tout $w \in \mathfrak{S}_n$. On observe que les polynômes symétriques élémentaires sont des polynômes symétriques. On note $A[t_1, \dots, t_n]^{\mathfrak{S}_n}$ l'ensemble des polynômes symétriques.

Lemme 5.3. $A[t_1, \dots, t_n]^{\mathfrak{S}_n}$ est un sous-anneau de $A[t_1, \dots, t_n]$.

Démonstration. Il est clair que $0, 1 \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$. Soient $f, g \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$. Alors, pour tout $w \in \mathfrak{S}_n$,

$$\begin{aligned} w \cdot (f - g) &= w \cdot f - w \cdot g = f - g, \\ w \cdot (fg) &= (w \cdot f)(w \cdot g) = fg, \end{aligned}$$

donc $f - g, fg \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$. Ceci montre que $A[t_1, \dots, t_n]^{\mathfrak{S}_n}$ est un sous-anneau de $A[t_1, \dots, t_n]$. \square

Théorème 5.4. Soit A un anneau intègre. Alors $A[t_1, \dots, t_n]^{\mathfrak{S}_n}$ est le sous-anneau de $A[t_1, \dots, t_n]$ engendré par s_1, \dots, s_n et A . En d'autres termes, on a

$$A[t_1, \dots, t_n]^{\mathfrak{S}_n} = A[s_1, \dots, s_n].$$

Le lemme suivant est un préliminaire à la démonstration du théorème 5.4.

Lemme 5.5. Soient A un anneau intègre et $f \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$. Supposons qu'il existe $h_1 \in A[t_1, \dots, t_n]$ tel que $f = h_1 t_1$. Alors il existe $g \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$ tel que $f = g t_1 \cdots t_n$.

Démonstration. On commence par démontrer par récurrence sur $k \in \{1, \dots, n\}$ qu'il existe $h_k \in A[t_1, \dots, t_n]$ tel que $f = h_k t_1 \cdots t_k$. Le cas $k = 1$ étant l'hypothèse du lemme, on peut supposer $1 < k \leq n$ plus l'hypothèse de récurrence, c'est-à-dire qu'il existe $h_{k-1} \in A[t_1, \dots, t_n]$ tel que $f = h_{k-1} t_1 \cdots t_{k-1}$. Posons $w = (k-1, k) \in \mathfrak{S}_n$. Soit $B = A[t_1, \dots, t_{k-1}, t_{k+1}, \dots, t_n]$. Soit

$$h_{k-1} = h_k t_k + r$$

la division de h_{k-1} par t_k dans $B[t_k]$. En multipliant cette expression par $t_1 \cdots t_{k-1}$ on obtient la division de f par t_k dans $B[t_k]$:

$$f = h_{k-1} t_1 \cdots t_{k-1} = (h_k t_1 \cdots t_{k-1}) t_k + r t_1 \cdots t_{k-1}.$$

Par ailleurs, en appliquant w à f on a

$$f = w \cdot f = ((w \cdot h_{k-1}) t_1 \cdots t_{k-2}) t_k.$$

L'unicité de la division implique que $r t_1 \cdots t_{k-1} = 0$, donc

$$f = h_k t_1 \cdots t_{k-1} t_k.$$

Posons $g = h_n$. Par ce qui précède, $f = g t_1 \cdots t_n$. Reste à montrer que $g \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$. Soit $w \in \mathfrak{S}_n$. Alors

$$g t_1 \cdots t_n = f = w \cdot f = (w \cdot g) t_1 \cdots t_n.$$

Comme $A[t_1, \dots, t_n]$ est intègre, cette égalité implique que $w \cdot g = g$. \square

Démonstration du théorème 5.4. Comme $s_1, \dots, s_n \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$, on a $A[s_1, \dots, s_n] \subset A[t_1, \dots, t_n]^{\mathfrak{S}_n}$. Reste à montrer que $A[t_1, \dots, t_n]^{\mathfrak{S}_n} \subset A[s_1, \dots, s_n]$. Pour cela on se donne $f \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$ et on montre qu'il existe $g \in A[X_1, \dots, X_n]$ tel que $f(t_1, \dots, t_n) = g(s_1, \dots, s_n)$, où X_1, \dots, X_n sont des indéterminées sur A .

On se donne X_1, \dots, X_n des indéterminées sur A . On définit le *poids* d'un monôme $P = X_1^{\mu_1} \dots X_n^{\mu_n}$ par

$$\text{poids } P = \mu_1 + 2\mu_2 + \dots + n\mu_n.$$

Si $g \in A[X_1, \dots, X_n]$ s'écrit $g = \sum_{\mu \in \mathbb{N}^n} a_\mu X^\mu$, on définit le *poids* de g par

$$\text{poids } g = \max\{\text{poids } X^\mu ; a_\mu \neq 0\}.$$

Comme $\deg s_k = k$ pour tout k on a

$$\deg g(s_1, \dots, s_n) \leq \text{poids } g.$$

Maintenant on se donne un polynôme $f \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$ de degré d et on montre par récurrence sur n qu'il existe $g \in A[X_1, \dots, X_n]$ tel que $\text{poids } g \leq d$ et $g(s_1, \dots, s_n) = f(t_1, \dots, t_n)$.

Supposons que $n = 1$. On a alors $A[t_1]^{\mathfrak{S}_1} = A[t_1]$ et $s_1 = t_1$, donc il suffit de prendre $g = f$ dans ce cas.

On suppose que $n > 1$ plus l'hypothèse de récurrence. Pour $h \in A[t_1, \dots, t_n]$ on pose

$$h_0 = h(t_1, \dots, t_{n-1}, 0) \in A[t_1, \dots, t_{n-1}].$$

On observe que, si $h \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$, alors $h_0 \in A[t_1, \dots, t_{n-1}]^{\mathfrak{S}_{n-1}}$. Par ailleurs, on a

$$(X - t_1)(X - t_2) \dots (X - t_{n-1})X = X^n - (s_1)_0 X^{n-1} + \dots + (-1)^{n-1} (s_{n-1})_0 X,$$

donc $(s_1)_0, \dots, (s_{n-1})_0$ sont les polynômes symétriques élémentaires en les variables t_1, \dots, t_{n-1} .

Maintenant on raisonne par récurrence sur d . Si $d = 0$, alors $f = a \in A$. On pose $g = a = f$. On a bien $\text{poids } g = 0 = d$ et $g(s_1, \dots, s_n) = a = f(t_1, \dots, t_n)$.

Supposons que $d > 0$ plus l'hypothèse de récurrence (sur d). Soit $f \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$ de degré d . On a $f_0 \in A[t_1, \dots, t_{n-1}]^{\mathfrak{S}_{n-1}}$ et $\deg f_0 \leq d$. Par hypothèse de récurrence (sur n) il existe $g_1 \in A[X_1, \dots, X_{n-1}]$ tel que $\text{poids } g_0 \leq d$ et

$$f_0 = f(t_1, \dots, t_{n-1}, 0) = g_1((s_1)_0, \dots, (s_{n-1})_0).$$

Posons

$$f_1 = f(t_1, \dots, t_{n-1}, t_n) - g_1(s_1, \dots, s_{n-1}).$$

On a $f_1 \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$ et $\deg f_1 \leq d$. Par ailleurs,

$$f_1(t_1, \dots, t_{n-1}, 0) = f_0(t_1, \dots, t_{n-1}) - g_1((s_1)_0, \dots, (s_{n-1})_0) = 0,$$

donc 0 est racine de f_1 vu comme polynôme dans $A[t_1, \dots, t_{n-1}][t_n]$. Par le théorème 1.9, on en déduit que t_n divise f_1 , c'est-à-dire qu'il existe $f'_1 \in A[t_1, \dots, t_{n-1}][t_n] = A[t_1, \dots, t_n]$ tel que $f_1 = f'_1 t_n$. On applique $w = (1, n)$ à ce polynôme et on a $f_1 = (w \cdot f'_1) t_1$. Par le lemme 5.5 il en résulte qu'il existe $f_2 \in A[t_1, \dots, t_n]^{\mathfrak{S}_n}$ tel que $f_1 = f_2 t_1 \cdots t_n$. Comme $\deg f_2 = \deg f_1 - n \leq d - 1 < d$, on peut appliquer la récurrence à f_2 et on obtient qu'il existe $g_2 \in A[X_1, \dots, X_n]$ tel que poids $g_2 \leq d - n$ et

$$f_2(t_1, \dots, t_n) = g_2(s_1, \dots, s_n).$$

Posons

$$g = g_1 + X_n g_2.$$

On a poids $g \leq d$ et

$$g(s_1, \dots, s_n) = g_1(s_1, \dots, s_{n-1}) + s_n g_2(s_1, \dots, s_n) = f - f_1 + t_1 \cdots t_n f_2 = f. \quad \square$$

Définition. Soient A, B deux anneaux (intègres) tels que $A \subset B$, et $b_1, \dots, b_n \in B$. Soient X_1, \dots, X_n des indéterminées sur A et $\varphi : A[X_1, \dots, X_n] \rightarrow B$ l'homomorphisme que envoie X_i sur b_i pour tout $i \in \{1, \dots, n\}$. On dit que b_1, \dots, b_n sont *algébriquement indépendants* sur A si φ est injectif.

Théorème 5.6. *Soit A un anneau commutatif intègre. Alors les polynômes symétriques élémentaires $s_1, \dots, s_n \in A[t_1, \dots, t_n]$ sont algébriquement indépendants.*

Démonstration. On raisonne par récurrence sur n . Si $n = 1$, alors par définition $s_1 = t_1$ est algébriquement indépendant (transcendant).

Supposons que $n \geq 2$ plus l'hypothèse de récurrence. Supposons qu'il existe $g \in A[X_1, \dots, X_n]$, $g \neq 0$, tel que $g(s_1, \dots, s_n) = 0$. On choisit g de degré minimal et on écrit

$$g = g_0 + g_1 X_n + \cdots + g_d X_n^d,$$

où $g_0, g_1, \dots, g_d \in A[X_1, \dots, X_{n-1}]$.

Supposons d'abord que $g_0 = 0$. Soit

$$h = g_1 + g_2 X_n + \cdots + g_d X_n^{d-1}.$$

Alors $g = X_n h$ et

$$\begin{aligned} s_n h(s_1, \dots, s_n) &= g(s_1, \dots, s_n) = 0 \\ \Rightarrow h(s_1, \dots, s_n) &= 0. \end{aligned}$$

Ceci contredit la minimalité du degré de g . Donc, on doit avoir $g_0 \neq 0$.

On pose $t_n = 0$ à l'égalité

$$0 = g(s_1, \dots, s_n) = g_0(s_1, \dots, s_{n-1}) + s_n g_1(s_1, \dots, s_{n-1}) + \dots + s_n^d g_d(s_1, \dots, s_{n-1})$$

et on obtient

$$0 = g_0((s_1)_0, \dots, (s_{n-1})_0) + (s_n)_0 g_1((s_1)_0, \dots, (s_{n-1})_0) + \dots \\ + (s_n)_0^d g_d((s_1)_0, \dots, (s_{n-1})_0) = g_0((s_1)_0, \dots, (s_{n-1})_0).$$

Ceci contredit l'hypothèse de récurrence (sur n). On en conclue qu'un tel g ne peut pas exister et s_1, \dots, s_n sont algébriquement indépendants. \square

Définition. Soit

$$\delta = \prod_{i < j} (t_i - t_j) \in A[t_1, \dots, t_n].$$

On vérifie facilement que

$$w \cdot \delta = \text{sign}(w) \delta$$

pour tout $w \in \mathfrak{S}_n$. En particulier

$$D = \delta^2 = \prod_{i < j} (t_i - t_j)^2$$

est un polynôme symétrique. Il s'appelle le *discriminant*.

Exemple. Si $n = 2$, alors

$$D = (t_1 - t_2)^2 = t_1^2 + t_2^2 - 2t_1 t_2 = (t_1 + t_2)^2 - 4t_1 t_2 = s_1^2 - 4s_2.$$

6 Résultant

Définition. Soient \mathbb{K} un corps et $f, g \in \mathbb{K}[X]$ deux polynômes non constants. Un *pgcd* de f et g est un polynôme $P \in \mathbb{K}[X]$ tel que

- (a) P divise f et g ;
- (b) si P' divise f et g , alors P' divise P .

Lemme 6.1. Soient \mathbb{K} un corps et $f, g \in \mathbb{K}[X]$ deux polynômes non constants. Alors $P \in \mathbb{K}[X]$ est un *pgcd* de f et g si et seulement si P engendre l'idéal (f, g) . En particulier :

- (1) f et g ont un *pgcd* ;

(2) si P et P' sont deux pgcd de f et g alors il existe une constante $c \in \mathbb{K} \setminus \{0\}$ telle que $P' = cP$;

(3) si P est un pgcd de f et g , alors il existe deux polynômes $A, B \in \mathbb{K}[X]$ tels que $P = Af + Bg$.

Démonstration. Exercice. □

Proposition 6.2. Soient \mathbb{K} un corps et $f, g \in \mathbb{K}[X]$ deux polynômes non constants. Soient n, m les degrés respectifs de f, g . Alors f et g ont un facteur commun non constant dans $\mathbb{K}[X]$ si et seulement s'il existe des polynômes $A, B \in \mathbb{K}[X]$ tels que

(a) $A \neq 0$ ou $B \neq 0$;

(b) $\deg A \leq m - 1$ et $\deg B \leq n - 1$;

(c) $Af + Bg = 0$.

Démonstration. Supposons que f, g ont un facteur commun non constant, h . Soient $f_1, g_1 \in \mathbb{K}[X]$ tels que $f = f_1h$ et $g = g_1h$. Posons $A = g_1$ et $B = -f_1$. Alors

(a) $A \neq 0$ et $B \neq 0$;

(b) $\deg A = \deg g_1 < \deg g = m$ et $\deg B = \deg f_1 < \deg f = n$;

(c) $Af + Bg = g_1f_1h - f_1g_1h = 0$.

Maintenant on suppose qu'il existe $A, B \in \mathbb{K}[X]$ vérifiant les conditions (a), (b) et (c) de la proposition. Par (a) on peut en toute généralité supposer que $B \neq 0$. On va raisonner par l'absurde et supposer que f et g sont premiers entre eux. Par le lemme 6.1 il existe $\tilde{A}, \tilde{B} \in \mathbb{K}[X]$ tels que $\tilde{A}f + \tilde{B}g = 1$. Par ailleurs,

$$Af + Bg = 0 \quad \Rightarrow \quad Bg = -Af.$$

Il s'en suit que

$$B = B1 = B(\tilde{A}f + \tilde{B}g) = \tilde{A}Bf + \tilde{B}Bg = \tilde{A}Bf - \tilde{B}Af = (\tilde{A}B - \tilde{B}A)f,$$

donc $\deg B \geq \deg f = n$, ce qui contredit (b). On en conclue que f et g ne sont pas premiers entre eux c'est-à-dire qu'ils ont un facteur commun non constant. □

Définition. Soient A un anneau intègre et $f, g \in A[X]$ deux polynômes non constants. On écrit

$$f = a_0X^n + a_1X^{n-1} + \cdots + a_n, \quad g = b_0X^m + b_1X^{m-1} + \cdots + b_m,$$

où $a_0 \neq 0$ et $b_0 \neq 0$. La *matrice de Sylvester* de (f, g) , notée $\text{Sylv}(f, g)$, est la matrice $(n+m) \times (n+m)$ suivante

$$\text{Sylv}(f, g) = \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & \vdots & b_1 & b_0 & \ddots & \vdots \\ \vdots & a_1 & \ddots & 0 & \vdots & b_1 & \ddots & 0 \\ a_n & \vdots & \ddots & a_0 & b_m & \vdots & \ddots & b_0 \\ 0 & a_n & & a_1 & 0 & b_m & & b_1 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_n & 0 & \cdots & 0 & b_m \end{pmatrix}$$

Le *résultant* de (f, g) , noté $\text{Res}(f, g)$, est le déterminant de la matrice de Sylvester,

$$\text{Res}(f, g) = \det(\text{Sylv}(f, g)).$$

Lemme 6.3. Soient A un anneau intègre et $a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m$ des indéterminées sur A . On pose $B = A[a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m]$ et on considère les polynômes

$$f = a_0X^n + a_1X^{n-1} + \cdots + a_n, \quad g = b_0X^m + b_1X^{m-1} + \cdots + b_m,$$

dans $B[X]$. Alors $\text{Res}(f, g)$ est un polynôme (en les variables a_i et b_j) homogène de degré $n+m$.

Démonstration. Exercice. □

Théorème 6.4. Soient \mathbb{K} un corps et $f, g \in \mathbb{K}[X]$ deux polynômes non constants. Alors f et g ont un facteur commun non constant si et seulement si $\text{Res}(f, g) = 0$.

Démonstration. On se donne deux polynômes non constants $f, g \in \mathbb{K}[X]$. On pose

$$f = a_0X^n + a_1X^{n-1} + \cdots + a_n, \quad g = b_0X^m + b_1X^{m-1} + \cdots + b_m,$$

où $a_0 \neq 0$ et $b_0 \neq 0$.

Supposons d'abord que f et g ont un facteur commun non constant. Par la proposition 6.2 il existe des polynômes $A, B \in \mathbb{K}[X]$ tels que

- (a) $A \neq 0$ ou $B \neq 0$;
- (b) $\deg A \leq m-1$ et $\deg B \leq n-1$;
- (c) $Af + Bg = 0$.

Posons

$$A = c_0X^{m-1} + \cdots + c_{m-1}, \quad B = d_0X^{n-1} + \cdots + d_{n-1}.$$

Alors

$$\begin{aligned} & Af + Bg = 0 \\ \Leftrightarrow & (a_0c_0 + b_0d_0)X^{n+m-1} + (a_1c_0 + a_0c_1 + b_1d_0 + b_0d_1)X^{n+m-2} \\ & \quad + \cdots + (a_nc_{m-1} + b_md_{n-1}) = 0 \\ \Leftrightarrow & \begin{cases} a_0c_0 + b_0d_0 = 0 \\ a_1c_0 + a_0c_1 + b_1d_0 + b_0d_1 = 0 \\ \cdots \\ a_nc_{m-1} + b_md_{n-1} = 0 \end{cases} \\ \Leftrightarrow & \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & \vdots & b_1 & b_0 & \ddots & \vdots \\ \vdots & a_1 & \ddots & 0 & \vdots & b_1 & \ddots & 0 \\ a_n & \vdots & \ddots & a_0 & b_m & \vdots & \ddots & b_0 \\ 0 & a_n & & a_1 & 0 & b_m & & b_1 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_n & 0 & \cdots & 0 & b_m \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{m-1} \\ d_0 \\ \vdots \\ d_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \end{aligned}$$

Cette dernière égalité implique qu'il existe un vecteur non nul $v \in \mathbb{K}^{n+m}$ tel que

$$\text{Sylv}(f, g) \cdot v = \vec{0},$$

d'où

$$\text{Res}(f, g) = \det(\text{Sylv}(f, g)) = 0.$$

Supposons maintenant que $\text{Res}(f, g) = 0$. Alors il existe un vecteur non nul $v \in \mathbb{K}^{n+m}$ tel que $\text{Sylv}(f, g) \cdot v = \vec{0}$. Posons,

$$v = (c_0, \dots, c_{m-1}, d_0, \dots, d_{n-1})^t.$$

Soient

$$A = c_0X^{m-1} + \cdots + c_{m-1}, \quad B = d_0X^{n-1} + \cdots + d_{n-1}.$$

Alors

- (a) $A \neq 0$ ou $B \neq 0$;
- (b) $\deg A \leq m - 1$ et $\deg B \leq n - 1$;
- (c) $Af + Bg = 0$.

Il en résulte par la proposition 6.2 que f et g ont un facteur commun non constant. \square

Exemple 1. Dans $\mathbb{Q}[X]$ on pose

$$f = 2X^2 + 3X + 1, \quad g = 7X^2 + X + 3.$$

Alors

$$\text{Res}(f, g) = \begin{vmatrix} 2 & 0 & 7 & 0 \\ 3 & 2 & 1 & 7 \\ 1 & 3 & 3 & 1 \\ 0 & 1 & 0 & 3 \end{vmatrix} = 153 \neq 0,$$

donc f et g sont premiers entre eux.

Exemple 2. Les polynômes

$$f = XY - 1, \quad g = X^2 + Y^2 - 4$$

sont premiers entre eux dans $\mathbb{Q}[X, Y]$. (Exercice.)

Théorème 6.5. Soient \mathbb{K} un corps et $a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m$ des indéterminées sur \mathbb{K} . Posons $A = \mathbb{K}[a_0, \dots, a_n, b_0, \dots, b_m]$. Soient

$$f = a_0X^n + a_1X^{n-1} + \dots + a_n, \quad g = b_0X^m + b_1X^{m-1} + \dots + b_m.$$

Il existe des polynômes $R, S \in A[X]$ tels que

- (a) $\deg R \leq m - 1$ et $\deg S \leq n - 1$;
- (b) $Rf + Sg = \text{Res}(f, g)$.

Le résultat suivant est un préliminaire à la démonstration du théorème 6.5.

Proposition 6.6 (Règle de Cramer). Soient \mathbb{K} un corps, $M \in \text{GL}(\mathbb{K}^n)$ une matrice inversible, et $v \in \mathbb{K}^n$ un vecteur. Alors l'unique solution de l'équation $Mx = v$ est donnée par

$$x_i = \frac{\det M_i}{\det M},$$

où M_i est la matrice obtenue à partir de M en remplaçant la i -ème colonne par v .

Démonstration. Exercice. \square

Démonstration du théorème 6.5. Notons \mathbb{F} le corps des fractions de A . Il est clair que f et g n'ont pas de facteur commun dans $\mathbb{F}[X]$, donc $\text{Res}(f, g) \neq 0$. Maintenant on se donne deux polynômes génériques $R, S \in A[X]$ tels que $\deg R \leq m - 1$ et $\deg S \leq n - 1$. On écrit

$$R = c_0X^{m-1} + \dots + c_{m-1}, \quad S = d_0X^{n-1} + \dots + d_{n-1}.$$

Alors

$$\begin{aligned}
& Rf + Sg = \text{Res}(f, g) \\
\Leftrightarrow & (a_0c_0 + b_0d_0)X^{n+m-1} + (a_1c_0 + a_0c_1 + b_1d_0 + b_0d_1)X^{n+m-2} \\
& \quad + \cdots + (a_nc_{m-1} + b_md_{n-1}) = \text{Res}(f, g) \\
\Leftrightarrow & \begin{cases} a_0c_0 + b_0d_0 & = 0 \\ a_1c_0 + a_0c_1 + b_1d_0 + b_0d_1 & = 0 \\ \cdots & \\ a_nc_{m-1} + b_md_{n-1} & = \text{Res}(f, g) \end{cases} \\
\Leftrightarrow & \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & \vdots & b_1 & b_0 & \ddots & \vdots \\ \vdots & a_1 & \ddots & 0 & \vdots & b_1 & \ddots & 0 \\ a_n & \vdots & \ddots & a_0 & b_m & \vdots & \ddots & b_0 \\ 0 & a_n & & a_1 & 0 & b_m & & b_1 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_n & 0 & \cdots & 0 & b_m \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{m-1} \\ d_0 \\ \vdots \\ d_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \text{Res}(f, g) \end{pmatrix} \quad (*)
\end{aligned}$$

Notons \bar{M}_i la matrice obtenue à partir de $\text{Sylv}(f, g)$ en remplaçant la i -ème colonne par $(0, \dots, 0, 1)^t$, et M_i la matrice obtenue à partir de $\text{Sylv}(f, g)$ en remplaçant la i -ème colonne par $(0, \dots, 0, \text{Res}(f, g))^t$. On remarque que

$$\begin{aligned}
\det M_i &= \text{Res}(f, g) \cdot \det \bar{M}_i, \\
\det \bar{M}_i &\in \mathbb{K}[a_0, \dots, a_n, b_0, \dots, b_m] = A.
\end{aligned}$$

Posons

$$\begin{aligned}
c_i &= \frac{\det M_{i+1}}{\text{Res}(f, g)} = \det \bar{M}_{i+1} \quad \text{si } 0 \leq i \leq m-1, \\
d_i &= \frac{\det M_{m+i+1}}{\text{Res}(f, g)} = \det \bar{M}_{m+i+1} \quad \text{si } 0 \leq i \leq n-1.
\end{aligned}$$

Par la proposition 6.6 le vecteur $v = (c_0, \dots, c_{m-1}, d_0, \dots, d_{n-1})^t$ vérifie l'égalité (*) donc, pour ces valeurs là, les polynômes R et S vérifient

(a) $\deg R \leq m-1$ et $\deg S \leq n-1$;

(b) $Rf + Sg = \text{Res}(f, g)$. □

Proposition 6.7. *Soit \mathbb{K} un corps algébriquement clos et $f, g \in \mathbb{K}[X]$ deux polynômes non constants. Alors f et g ont une racine commune si et seulement si $\text{Res}(f, g) = 0$.*

Démonstration. Supposons que f et g ont une racine commune, $a \in \mathbb{K}$. Alors f et g ont un facteur non constant commun, $X - a$, donc, par le théorème 6.4, $\text{Res}(f, g) = 0$.

Réciproquement, si $\text{Res}(f, g) = 0$, par le théorème 6.4 f et g ont un facteur non constant commun, h . Comme \mathbb{K} est algébriquement clos, h a une racine, a . Alors a est racine commune de f et g . \square

Corollaire 6.8. Soient \mathbb{K} un corps algébriquement clos et $f \in \mathbb{K}[X]$ un polynôme de degré ≥ 2 . Alors f a une racine multiple si et seulement si $\text{Res}(f, f') = 0$. \square

Exemple. Soit $f = aX^2 + bX + c$ un polynôme de degré 2 à coefficients dans \mathbb{K} . Alors

$$\text{Res}(f, f') = \begin{vmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{vmatrix} = -a(b^2 - 4ac),$$

donc f a une racine multiple si et seulement si $b^2 - 4ac = 0$.

Maintenant on se donne des indéterminées $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m, u_0, v_0$ sur \mathbb{Z} et on pose

$$\begin{aligned} A &= \mathbb{Z}[\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m, u_0, v_0] = \mathbb{Z}[\vec{\alpha}, \vec{\beta}, u_0, v_0], \\ f &= u_0(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n) \in A[X], \\ g &= v_0(X - \beta_1)(X - \beta_2) \cdots (X - \beta_m) \in A[X], \\ \Phi(\vec{\alpha}, \vec{\beta}, u_0, v_0) &= \text{Res}(f, g) \in A. \end{aligned}$$

Lemme 6.9. $\Phi(\vec{\alpha}, \vec{\beta}, u_0, v_0)$ est divisible par $\alpha_i - \beta_j$ pour tous $i \in \{1, \dots, n\}$ et $j \in \{1, \dots, m\}$.

Démonstration. On peut supposer en toute généralité que $i = j = 1$. On effectue la division de $\Phi(\vec{\alpha}, \vec{\beta}, u_0, v_0)$ par $(\alpha_1 - \beta_1)$ par rapport à l'indéterminée α_1 :

$$\Phi(\vec{\alpha}, \vec{\beta}, u_0, v_0) = (\alpha_1 - \beta_1)Q(\vec{\alpha}, \vec{\beta}, u_0, v_0) + R(\alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m, u_0, v_0). \quad (1)$$

On choisit $\lambda_2, \dots, \lambda_n, \mu_1, \mu_2, \dots, \mu_m, a_0, b_0 \in \mathbb{C}$ avec $a_0 \neq 0$ et $b_0 \neq 0$, et on considère la spécialisation

$$\begin{aligned} \alpha_i &= \lambda_i \text{ pour } i \in \{2, \dots, n\}, & \beta_j &= \mu_j \text{ pour } j \in \{1, \dots, m\}, \\ u_0 &= a_0, & v_0 &= b_0, & \alpha_1 &= \mu_1. \end{aligned}$$

Avec cette spécialisation f et g ont une racine commune, donc

$$\text{Res}(f, g) = \Phi(\mu_1, \lambda_2, \dots, \lambda_n, \mu_1, \mu_2, \dots, \mu_m, a_0, b_0) = 0.$$

On applique la spécialisation à (1) et on obtient

$$\begin{aligned} 0 &= (\mu_1 - \mu_1)Q(\mu_1, \lambda_2, \dots, \lambda_n, \mu_1, \mu_2, \dots, \mu_m, a_0, b_0) + R(\lambda_2, \dots, \lambda_n, \mu_1, \mu_2, \dots, \mu_m, a_0, b_0) \\ &= R(\lambda_2, \dots, \lambda_n, \mu_1, \mu_2, \dots, \mu_m, a_0, b_0). \end{aligned}$$

Cette égalité étant vraie quelque soient $\lambda_2, \dots, \lambda_n, \mu_1, \mu_2, \dots, \mu_m, a_0, b_0$, on en déduit que $R = 0$, donc

$$\Phi(\vec{\alpha}, \vec{\beta}, u_0, v_0) = (\alpha_1 - \beta_1)Q(\vec{\alpha}, \vec{\beta}, u_0, v_0). \quad \square$$

Lemme 6.10. *La partie homogène de plus haut degré en les β_1, \dots, β_m de $\Phi(\vec{\alpha}, \vec{\beta}, u_0, v_0)$ vaut*

$$(-1)^{nm} u_0^m v_0^n (\beta_1 \beta_2 \cdots \beta_m)^n.$$

Démonstration. Exercice. □

Théorème 6.11. *Avec les notations ci-dessus :*

$$\Phi(\vec{\alpha}, \vec{\beta}, u_0, v_0) = u_0^m v_0^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j) = u_0^m \prod_{i=1}^n g(\alpha_i) = (-1)^{nm} v_0^n \prod_{j=1}^m f(\beta_j).$$

Démonstration. Par le lemme 6.9 $\alpha_i - \beta_j$ divise $\Phi(\vec{\alpha}, \vec{\beta}, u_0, v_0)$ pour tous $i \in \{1, \dots, n\}$ et $j \in \{1, \dots, m\}$, ces éléments sont 2 à 2 premiers entre eux, et $A = \mathbb{Z}[\vec{\alpha}, \vec{\beta}, u_0, v_0]$ est factoriel, donc il existe $F \in A$ tel que

$$\Phi(\vec{\alpha}, \vec{\beta}, u_0, v_0) = F \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j).$$

Par le lemme 6.10 la partie homogène de plus haut degré en les β_1, \dots, β_m de $\Phi(\vec{\alpha}, \vec{\beta}, u_0, v_0)$ vaut

$$(-1)^{nm} u_0^m v_0^n (\beta_1 \beta_2 \cdots \beta_m)^n.$$

Par ailleurs, on observe que la partie homogène de plus haut degré en les β_1, \dots, β_m de $\prod_{i,j} (\alpha_i - \beta_j)$ vaut

$$(-1)^{nm} (\beta_1 \beta_2 \cdots \beta_m)^n.$$

On en déduit que $F = u_0^m v_0^n$, donc

$$\Phi(\vec{\alpha}, \vec{\beta}, u_0, v_0) = u_0^m v_0^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j).$$

Les deux autres égalités découlent directement de la première. □

Corollaire 6.12. *Soient A un anneau intègre et $f, g \in A[X]$ deux polynômes non constants. Notons n, m les degrés de f, g , respectivement.*

(1) Supposons que f s'écrit sous la forme

$$f = a_0 \prod_{i=1}^n (X - \lambda_i),$$

où $\lambda_1, \dots, \lambda_n, a_0 \in A$, $a_0 \neq 0$. Alors

$$\text{Res}(f, g) = a_0^m \prod_{i=1}^n g(\lambda_i).$$

(2) Supposons que f et g s'écrivent sous la forme

$$f = a_0 \prod_{i=1}^n (X - \lambda_i), \quad g = b_0 \prod_{j=1}^m (X - \mu_j),$$

où $\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_m, a_0, b_0 \in A$, $a_0 \neq 0$ et $b_0 \neq 0$. Alors

$$\text{Res}(f, g) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j).$$

Démonstration. Exercice. □

Définition. Soient \mathbb{K} un corps algébriquement clos et $f \in \mathbb{K}[X]$ un polynôme de degré $n \geq 2$. On écrit f sous la forme

$$f = a_0 \prod_{i=1}^n (X - \lambda_i),$$

où $\lambda_1, \dots, \lambda_n, a_0 \in \mathbb{K}$, $a_0 \neq 0$. Le *discriminant* de f est défini par

$$\text{Disc}(f) = \prod_{i < j} (\lambda_i - \lambda_j)^2.$$

Remarque. Il est clair que f a une racine multiple si et seulement si $\text{Disc}(f) = 0$. Par ailleurs, on sait que f a une racine multiple si et seulement si $\text{Res}(f, f') = 0$.

Proposition 6.13. Soient \mathbb{K} un corps algébriquement clos et $f \in \mathbb{K}[X]$ un polynôme unitaire de degré $n \geq 2$. Alors

$$\text{Res}(f, f') = (-1)^{\frac{n(n-1)}{2}} \text{Disc}(f).$$

Démonstration. On écrit f sous la forme

$$f = \prod_{i=1}^n (X - \lambda_i),$$

où $\lambda_1, \dots, \lambda_n \in \mathbb{K}$. On a

$$f' = \sum_{i=1}^n \prod_{j \neq i} (X - \lambda_j),$$

donc, pour tout $k \in \{1, \dots, n\}$,

$$f'(\lambda_k) = \sum_{i=1}^n \prod_{j \neq i} (\lambda_k - \lambda_j) = \prod_{j \neq k} (\lambda_k - \lambda_j),$$

d'où

$$\begin{aligned} \text{Res}(f, f') &= \prod_{k=1}^n f'(\lambda_k) = \prod_{k=1}^n \prod_{j \neq k} (\lambda_k - \lambda_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{k < j} (\lambda_k - \lambda_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \text{Disc}(f). \quad \square \end{aligned}$$

Partie 2 : Extensions de corps

7 Extensions algébriques

Définition. Si \mathbb{E} est un corps et \mathbb{F} un sous-corps de \mathbb{E} on dit que $\mathbb{F} \subset \mathbb{E}$ est une *extension de corps*. On observe que, si $\mathbb{F} \subset \mathbb{E}$ est une extension de corps, \mathbb{E} est un espace vectoriel sur \mathbb{F} . La dimension de \mathbb{E} vu comme espace vectoriel sur \mathbb{F} s'appelle le *degré* de l'extension et se note $[\mathbb{E} : \mathbb{F}]$. On dit que l'extension est de *degré fini* si $[\mathbb{E} : \mathbb{F}]$ est fini.

Définition. Soient $\mathbb{F} \subset \mathbb{E}$ une extension de corps et $\alpha \in \mathbb{E}$. On dit que α est *algébrique* sur \mathbb{F} s'il existe un polynôme non nul $f \in \mathbb{F}[X]$ tel que $f(\alpha) = 0$. Autrement on dit que α est *transcendant* sur \mathbb{F} .

Remarque-définition. Soient $\mathbb{F} \subset \mathbb{E}$ une extension et $\alpha \in \mathbb{E}$ un élément algébrique sur \mathbb{F} . Le noyau de l'homomorphisme

$$\begin{aligned} \psi : \mathbb{F}[X] &\rightarrow \mathbb{E} \\ f &\mapsto f(\alpha) \end{aligned}$$

est non trivial. Comme $\mathbb{F}[X]$ est principal, il existe un polynôme non nul $p \in \mathbb{F}[X]$, unique à multiplication par un scalaire près, tel que $\text{Ker } \psi = (p)$. L'homomorphisme ψ induit un homomorphisme injectif

$$\bar{\psi} : \mathbb{F}[X]/(p) \rightarrow \mathbb{E}.$$

Comme \mathbb{E} est un corps et $\bar{\psi}$ est injectif, $\mathbb{F}[X]/(p)$ doit être intègre, donc p est premier. Ce polynôme p s'appelle le *polynôme minimal* de α .

Définition. On dit qu'une extension $\mathbb{F} \subset \mathbb{E}$ est *algébrique* si tout élément de \mathbb{E} est algébrique sur \mathbb{F} .

Proposition 7.1. *Toute extension de corps de degré fini est algébrique.*

Démonstration. Soit $\mathbb{F} \subset \mathbb{E}$ une extension de degré fini. Posons $n = [\mathbb{E} : \mathbb{F}]$. Soit $\alpha \in \mathbb{E}$. Le cardinal de l'ensemble $\{1, \alpha, \dots, \alpha^n\}$ est $n + 1$, donc cet ensemble est lié, donc il existe $a_0, a_1, \dots, a_n \in \mathbb{F}$ non tous nuls tels que

$$a_0 + a_1\alpha + \dots + a_n\alpha^n = 0.$$

Posons

$$f = a_0 + a_1X + \dots + a_nX^n.$$

Alors f est un polynôme non nul dans $\mathbb{F}[X]$ et $f(\alpha) = 0$. Ceci montre que α est algébrique sur \mathbb{F} . \square

Proposition 7.2. *Soient $\mathbb{K}, \mathbb{F}, \mathbb{E}$ des corps tels que $\mathbb{K} \subset \mathbb{F} \subset \mathbb{E}$. Soient \mathcal{X} une base de \mathbb{F} vu comme espace vectoriel sur \mathbb{K} et \mathcal{Y} une base de \mathbb{E} vu comme espace vectoriel sur \mathbb{F} . Alors $\{xy \mid x \in \mathcal{X} \text{ et } y \in \mathcal{Y}\}$ est une base de \mathbb{E} vu comme espace vectoriel sur \mathbb{K} . En particulier*

$$[\mathbb{E} : \mathbb{K}] = [\mathbb{E} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{K}].$$

Démonstration. Soit $\gamma \in \mathbb{E}$. Comme \mathcal{Y} est une base de \mathbb{E} vu comme espace vectoriel sur \mathbb{F} , il existe $n \in \mathbb{N}$, $y_1, \dots, y_n \in \mathcal{Y}$ et $\beta_1, \dots, \beta_n \in \mathbb{F}$ tels que

$$\gamma = \sum_{i=1}^n \beta_i y_i.$$

Comme \mathcal{X} est une base de \mathbb{F} vu comme espace vectoriel sur \mathbb{K} , il existe $m \in \mathbb{N}$, $x_1, \dots, x_m \in \mathcal{X}$ et, pour tout $i \in \{1, \dots, n\}$, $\alpha_{i,1}, \dots, \alpha_{i,m} \in \mathbb{K}$, tels que

$$\beta_i = \sum_{j=1}^m \alpha_{i,j} x_j.$$

D'où

$$\gamma = \sum_{i=1}^n \sum_{j=1}^m \alpha_{i,j} x_j y_i.$$

Ceci montre que $\{xy \mid x \in \mathcal{X} \text{ et } y \in \mathcal{Y}\}$ engendre \mathbb{E} vu comme espace vectoriel sur \mathbb{K} .

Supposons donnés $n, m \in \mathbb{N}$, $y_1, \dots, y_n \in \mathcal{Y}$, $x_1, \dots, x_m \in \mathcal{X}$, et $\{\alpha_{i,j}; i \in \{1, \dots, n\} \text{ et } j \in \{1, \dots, m\}\}$ tels que

$$\sum_{i=1}^n \sum_{j=1}^m \alpha_{i,j} x_j y_i = 0.$$

Pour $i \in \{1, \dots, n\}$ on pose

$$\beta_i = \sum_{j=1}^m \alpha_{i,j} x_j \in \mathbb{F}.$$

On a

$$\sum_{i=1}^n \beta_i y_i = 0$$

et \mathcal{Y} est une base de \mathbb{E} vu comme espace vectoriel sur \mathbb{F} , donc

$$\beta_i = \sum_{j=1}^m \alpha_{i,j} x_j = 0$$

pour tout $i \in \{1, \dots, n\}$. Comme \mathcal{X} est une base de \mathbb{F} vu comme espace vectoriel sur \mathbb{K} , cette dernière égalité implique que $\alpha_{i,j} = 0$ pour tous $i \in \{1, \dots, n\}$ et $j \in \{1, \dots, m\}$. Ceci montre que $\{xy \mid x \in \mathcal{X} \text{ et } y \in \mathcal{Y}\}$ est libre. \square

Corollaire 7.3. *Soient $\mathbb{K}, \mathbb{F}, \mathbb{E}$ trois corps tels que $\mathbb{K} \subset \mathbb{F} \subset \mathbb{E}$. Alors $\mathbb{K} \subset \mathbb{E}$ est une extension de degré fini si et seulement si $\mathbb{K} \subset \mathbb{F}$ et $\mathbb{F} \subset \mathbb{E}$ sont des extensions de degré fini.* \square

Notation. Soient $\mathbb{F} \subset \mathbb{E}$ une extension de corps et $\alpha \in \mathbb{E}$. On note $\mathbb{F}(\alpha)$ le plus petit sous-corps de \mathbb{E} contenant \mathbb{F} et α .

Lemme 7.4. *Soient $\mathbb{F} \subset \mathbb{E}$ une extension de corps et $\alpha \in \mathbb{E}$. Alors $\mathbb{F}(\alpha)$ est formé des éléments de la forme $\frac{f(\alpha)}{g(\alpha)}$ où $f, g \in \mathbb{F}[X]$, $g(\alpha) \neq 0$.*

Démonstration. Exercice \square

Proposition 7.5. *Soient $\mathbb{F} \subset \mathbb{E}$ une extension de corps et $\alpha \in \mathbb{E}$ un élément algébrique sur \mathbb{F} .*

- (1) $F(\alpha) = F[\alpha]$.
- (2) Soit p le polynôme minimal de α . Alors $F[\alpha] \simeq F[X]/(p)$.
- (3) $[F(\alpha) : \mathbb{F}] = \deg p$.

Démonstration. Rappelons l'homomorphisme

$$\begin{aligned} \psi : \mathbb{F}[X] &\rightarrow \mathbb{E} \\ f &\mapsto f(\alpha) \end{aligned}$$

Rappelons encore que $\text{Ker } \psi = (p)$. Remarquons que l'égalité $f(\alpha) = 0$ équivaut à $f \in \text{Ker } \psi$, c'est-à-dire à f est divisible par p .

Soit $\beta \in \mathbb{F}(\alpha)$. Par le Lemme 7.4 il existe $g_1, g_2 \in \mathbb{F}[X]$ tels que $g_2(\alpha) \neq 0$ et $\beta = \frac{g_1(\alpha)}{g_2(\alpha)}$. Par les observations précédentes, Le fait que $g_2(\alpha) \neq 0$ implique que p ne divise pas g_2 donc que g_2 et p sont premiers entre eux car p est premier. On peut donc trouver des polynômes $h_1, h_2 \in \mathbb{F}[X]$ tels que

$$h_1 p + h_2 g_2 = 1$$

En spécialisant cette égalité en $X = \alpha$ on obtient

$$\begin{aligned} 1 &= h_1(\alpha)p(\alpha) + h_2(\alpha)g_2(\alpha) = h_2(\alpha)g_2(\alpha) \\ \Rightarrow h_2(\alpha) &= \frac{1}{g_2(\alpha)} \\ \Rightarrow \beta &= \frac{g_1(\alpha)}{g_2(\alpha)} = g_1(\alpha)h_2(\alpha) \in \mathbb{F}[\alpha]. \end{aligned}$$

Ceci montre que $\mathbb{F}(\alpha) \subset \mathbb{F}[\alpha]$. L'inclusion $\mathbb{F}[\alpha] \subset \mathbb{F}(\alpha)$ est triviale.

On a $\text{Im } \psi = \mathbb{F}[\alpha] = \mathbb{F}(\alpha)$ et $\text{Ker } \psi = (p)$, donc

$$\mathbb{F}[X]/(p) = \mathbb{F}[X]/\text{Ker } \psi \simeq \text{Im } \psi = \mathbb{F}(\alpha).$$

Pour $f \in \mathbb{F}[X]$ on note $[f]$ la classe de f dans $\mathbb{F}[X]/(p) \simeq \mathbb{F}(\alpha)$. Posons $d = \deg p$. On va montrer que $\{1, [X], \dots, [X^{d-1}]\}$ est une base de $\mathbb{F}[X]/(p)$. Ceci implique que $d = [\mathbb{F}(\alpha), \mathbb{F}]$.

Soit $f \in \mathbb{F}[X]$. Soit $f = qp + r$ la division de f par p . Comme $\deg r < d$, on peut écrire r sous la forme

$$r = a_0 + a_1 X + \dots + a_{d-1} X^{d-1},$$

avec $a_0, a_1, \dots, a_{d-1} \in \mathbb{F}$. Alors

$$[f] = [r] = a_0 [1] + a_1 [X] + \dots + a_{d-1} [X^{d-1}].$$

Ceci montre que $\{1, [X], \dots, [X^{d-1}]\}$ engendre $\mathbb{F}[X]/(p)$.

Soient $a_0, a_1, \dots, a_{d-1} \in \mathbb{F}$ tels que

$$a_0 1 + a_1 [X] + \dots + a_{d-1} [X^{d-1}] = 0.$$

Posons

$$r = a_0 + a_1X + \cdots + a_{d-1}X^{d-1} \in \mathbb{F}[X].$$

On a

$$[r] = a_0 1 + a_1 [X] + \cdots + a_{d-1} [X^{d-1}] = 0,$$

donc p divise r , donc $r = 0$ car $\deg r < d = \deg p$, donc $a_0 = a_1 = \cdots = a_{d-1} = 0$. Ceci montre que $\{1, [X], \dots, [X^{d-1}]\}$ est libre. \square

Corollaire 7.6. *Soient $\mathbb{F} \subset \mathbb{E}$ une extension de corps et $\alpha \in \mathbb{E}$. Alors α est algébrique sur \mathbb{F} si et seulement si l'extension $\mathbb{F} \subset \mathbb{F}(\alpha)$ est de degré fini.*

Démonstration. Si α est algébrique alors $\mathbb{F} \subset \mathbb{F}(\alpha)$ est de degré fini par la proposition 7.5 (3). Réciproquement, si $\mathbb{F} \subset \mathbb{F}(\alpha)$ est de degré fini, alors α est algébrique par la proposition 7.1 (car $\alpha \in \mathbb{F}(\alpha)$). \square

Définition. Soient $\mathbb{F} \subset \mathbb{E}$ une extension de corps et $\alpha_1, \dots, \alpha_n \in \mathbb{E}$. On note $\mathbb{F}(\alpha_1, \dots, \alpha_n)$ le plus petit sous-corps de \mathbb{E} contenant \mathbb{F} et $\alpha_1, \dots, \alpha_n$. On dit que l'extension $\mathbb{F} \subset \mathbb{E}$ est de *type fini* s'il existe un nombre fini d'éléments $\alpha_1, \dots, \alpha_n \in \mathbb{E}$ tels que $\mathbb{E} = \mathbb{F}(\alpha_1, \dots, \alpha_n)$.

Lemme 7.7. *Soient $\mathbb{F} \subset \mathbb{E}$ une extension de corps et $\alpha_1, \dots, \alpha_n \in \mathbb{E}$. Alors $\mathbb{F}(\alpha_1, \dots, \alpha_n)$ est formé des fractions de la forme $\frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)}$ avec $f, g \in \mathbb{F}[X_1, \dots, X_n]$ et $g(\alpha_1, \dots, \alpha_n) \neq 0$.*

Démonstration. Exercice. \square

Proposition 7.8. *Toute extension de degré fini est de type fini. La réciproque est fausse.*

Démonstration. Exercice. \square

Proposition 7.9. *Soient $\mathbb{F} \subset \mathbb{E}$ une extension de type fini et $\alpha_1, \dots, \alpha_n \in \mathbb{E}$ tels que $\mathbb{E} = \mathbb{F}(\alpha_1, \dots, \alpha_n)$. Alors $\mathbb{F} \subset \mathbb{E}$ est de degré fini si et seulement si $\alpha_1, \dots, \alpha_n$ sont algébriques sur \mathbb{F} .*

Démonstration. Supposons que l'extension $\mathbb{F} \subset \mathbb{E}$ est de degré fini. Par la proposition 7.1 il en découle que l'extension est algébrique, donc $\alpha_1, \dots, \alpha_n$ sont algébriques car $\alpha_1, \dots, \alpha_n \in \mathbb{E}$.

Maintenant on suppose que $\alpha_1, \dots, \alpha_n$ sont algébriques sur \mathbb{F} et on démontre que l'extension $\mathbb{F} \subset \mathbb{E}$ est de degré fini. On raisonne par récurrence sur n . Le cas $n = 1$ suit de la proposition 7.5. Supposons que $n \geq 2$ plus l'hypothèse de récurrence. Par hypothèse de récurrence l'extension $\mathbb{F} \subset \mathbb{F}(\alpha_1, \dots, \alpha_{n-1})$ est de degré fini. Il est clair que le fait que α_n soit algébrique sur \mathbb{F} implique qu'il est algébrique sur $\mathbb{F}(\alpha_1, \dots, \alpha_{n-1})$, donc, encore par la proposition 7.5, l'extension

$$\mathbb{F}(\alpha_1, \dots, \alpha_{n-1}) \subset \mathbb{F}(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) = \mathbb{F}(\alpha_1, \dots, \alpha_{n-1}, \alpha_n) = \mathbb{E}$$

est de degré fini. On en conclue par le corollaire 7.3 que l'extension $\mathbb{F} \subset \mathbb{E}$ est de degré fini. \square

Notation. Soient $\mathbb{F}_1, \mathbb{F}_2, \mathbb{E}$ 3 corps tels que $\mathbb{F}_1 \subset \mathbb{E}$ et $\mathbb{F}_2 \subset \mathbb{E}$. Alors $\mathbb{F}_1\mathbb{F}_2$ désigne le plus petit sous-corps de \mathbb{E} contenant $\mathbb{F}_1 \cup \mathbb{F}_2$.

Lemme 7.10. Soient $\mathbb{F}_1, \mathbb{F}_2, \mathbb{E}$ 3 corps tels que $\mathbb{F}_1 \subset \mathbb{E}$ et $\mathbb{F}_2 \subset \mathbb{E}$. Soit $\beta \in \mathbb{F}_1\mathbb{F}_2$. Alors il existe un nombre fini d'éléments $\alpha_1, \dots, \alpha_n \in \mathbb{F}_2$ tels que $\beta \in \mathbb{F}_1(\alpha_1, \dots, \alpha_n)$.

Démonstration. Posons

$$U = \{\beta \in \mathbb{E} ; \text{il existe } n \in \mathbb{N} \text{ et } \alpha_1, \dots, \alpha_n \in \mathbb{F}_2 \text{ tels que } \beta \in \mathbb{F}_1(\alpha_1, \dots, \alpha_n)\}.$$

On a clairement les inclusions

$$\mathbb{F}_1 \subset U, \mathbb{F}_2 \subset U, U \subset \mathbb{F}_1\mathbb{F}_2.$$

Donc, pour démontrer que $U = \mathbb{F}_1\mathbb{F}_2$, il suffit de montrer que U est un sous-corps de \mathbb{E} .

On a $1, 0 \in \mathbb{F}_1$ et $\mathbb{F}_1 \subset U$, donc $1, 0 \in U$. Soient $\beta_1, \beta_2 \in U$. Il existe $n \in \mathbb{N}$ et $\alpha_1, \dots, \alpha_n \in \mathbb{F}_2$ tels que $\beta_1 \in \mathbb{F}_1(\alpha_1, \dots, \alpha_n)$. De même, il existe $m \in \mathbb{N}$ et $\alpha'_1, \dots, \alpha'_m \in \mathbb{F}_2$ tels que $\beta_2 \in \mathbb{F}_1(\alpha'_1, \dots, \alpha'_m)$. On a

$$\beta_1 - \beta_2 \in \mathbb{F}_1(\alpha_1, \dots, \alpha_n, \alpha'_1, \dots, \alpha'_m),$$

donc $\beta_1 - \beta_2 \in U$. De même, si $\beta_1 \neq 0$ et $\beta_2 \neq 0$, on a

$$\beta_1\beta_2^{-1} \in \mathbb{F}_1(\alpha_1, \dots, \alpha_n, \alpha'_1, \dots, \alpha'_m),$$

donc $\beta_1\beta_2^{-1} \in U$. Ceci montre que U est un sous-corps de \mathbb{E} . \square

Proposition 7.11.

- (1) Soient $\mathbb{K}, \mathbb{F}, \mathbb{E}$ trois corps tels que $\mathbb{K} \subset \mathbb{F} \subset \mathbb{E}$. Alors $\mathbb{K} \subset \mathbb{E}$ est une extension de degré fini si et seulement si $\mathbb{K} \subset \mathbb{F}$ et $\mathbb{F} \subset \mathbb{E}$ sont des extensions de degré fini.
- (2) Soient $\mathbb{K}, \mathbb{F}_1, \mathbb{F}_2, \mathbb{E}$ quatre corps tels que $\mathbb{K} \subset \mathbb{F}_1 \subset \mathbb{E}$ et $\mathbb{K} \subset \mathbb{F}_2 \subset \mathbb{E}$. Si $\mathbb{K} \subset \mathbb{F}_2$ est une extension de degré fini, alors $\mathbb{F}_1 \subset \mathbb{F}_1\mathbb{F}_2$ est une extension de degré fini.
- (3) Soient $\mathbb{K}, \mathbb{F}_1, \mathbb{F}_2, \mathbb{E}$ quatre corps tels que $\mathbb{K} \subset \mathbb{F}_1 \subset \mathbb{E}$ et $\mathbb{K} \subset \mathbb{F}_2 \subset \mathbb{E}$. Si $\mathbb{K} \subset \mathbb{F}_1$ et $\mathbb{K} \subset \mathbb{F}_2$ sont des extensions de degré fini, alors $\mathbb{K} \subset \mathbb{F}_1\mathbb{F}_2$ est une extension de degré fini.

Démonstration. La partie (1) est déjà connue (voir le corollaire 7.3). La partie (3) découle des parties (1) et (2). En effet, si $\mathbb{K} \subset \mathbb{F}_1$ et $\mathbb{K} \subset \mathbb{F}_2$ sont des extensions de degré fini, alors $\mathbb{F}_1 \subset \mathbb{F}_1\mathbb{F}_2$ est une extension de degré fini par (2) et donc, par (1), $\mathbb{K} \subset \mathbb{F}_1\mathbb{F}_2$ est une extension de degré fini. Reste à démontrer la partie (2).

Supposons que $\mathbb{K} \subset \mathbb{F}_2$ est une extension de degré fini. Par la proposition 7.8, $\mathbb{K} \subset \mathbb{F}_2$ est de type fini, donc il existe $\alpha_1, \dots, \alpha_n \in \mathbb{F}_2$ tels que $\mathbb{F}_2 = \mathbb{K}(\alpha_1, \dots, \alpha_n)$. Par la proposition 7.9 $\alpha_1, \dots, \alpha_n$ sont algébriques sur \mathbb{K} . Comme $\mathbb{F}_1 \subset \mathbb{F}_1\mathbb{F}_2$ et $\alpha_1, \dots, \alpha_n \in \mathbb{F}_2 \subset \mathbb{F}_1\mathbb{F}_2$, on a $\mathbb{F}_1(\alpha_1, \dots, \alpha_n) \subset \mathbb{F}_1\mathbb{F}_2$. Par ailleurs $\mathbb{F}_1 \subset \mathbb{F}_1(\alpha_1, \dots, \alpha_n)$ et $\mathbb{F}_2 = \mathbb{K}(\alpha_1, \dots, \alpha_n) \subset \mathbb{F}_1(\alpha_1, \dots, \alpha_n)$, donc $\mathbb{F}_1\mathbb{F}_2 \subset \mathbb{F}_1(\alpha_1, \dots, \alpha_n)$. D'où $\mathbb{F}_1\mathbb{F}_2 = \mathbb{F}_1(\alpha_1, \dots, \alpha_n)$. Comme $\alpha_1, \dots, \alpha_n$ sont algébriques sur \mathbb{K} , ils sont algébriques sur \mathbb{F}_1 , donc, par la proposition 7.9, $\mathbb{F}_1 \subset \mathbb{F}_1(\alpha_1, \dots, \alpha_n) = \mathbb{F}_1\mathbb{F}_2$ est de degré fini. \square

Proposition 7.12.

- (1) Soient $\mathbb{K}, \mathbb{F}, \mathbb{E}$ trois corps tels que $\mathbb{K} \subset \mathbb{F} \subset \mathbb{E}$. Alors $\mathbb{K} \subset \mathbb{E}$ est une extension algébrique si et seulement si $\mathbb{K} \subset \mathbb{F}$ et $\mathbb{F} \subset \mathbb{E}$ sont des extensions algébriques.
- (2) Soient $\mathbb{K}, \mathbb{F}_1, \mathbb{F}_2, \mathbb{E}$ quatre corps tels que $\mathbb{K} \subset \mathbb{F}_1 \subset \mathbb{E}$ et $\mathbb{K} \subset \mathbb{F}_2 \subset \mathbb{E}$. Si $\mathbb{K} \subset \mathbb{F}_2$ est une extension algébrique, alors $\mathbb{F}_1 \subset \mathbb{F}_1\mathbb{F}_2$ est une extension algébrique.
- (3) Soient $\mathbb{K}, \mathbb{F}_1, \mathbb{F}_2, \mathbb{E}$ quatre corps tels que $\mathbb{K} \subset \mathbb{F}_1 \subset \mathbb{E}$ et $\mathbb{K} \subset \mathbb{F}_2 \subset \mathbb{E}$. Si $\mathbb{K} \subset \mathbb{F}_1$ et $\mathbb{K} \subset \mathbb{F}_2$ sont des extensions algébriques, alors $\mathbb{K} \subset \mathbb{F}_1\mathbb{F}_2$ est une extension algébrique.

Démonstration.

Démonstration de (1). Soient $\mathbb{K}, \mathbb{F}, \mathbb{E}$ trois corps tels que $\mathbb{K} \subset \mathbb{F} \subset \mathbb{E}$. Supposons que $\mathbb{K} \subset \mathbb{E}$ est une extension algébrique. Soit $\alpha \in \mathbb{F}$. On a $\alpha \in \mathbb{E}$, donc α est algébrique sur \mathbb{K} . Ceci montre que $\mathbb{K} \subset \mathbb{F}$ est une extension algébrique. Soit $\beta \in \mathbb{E}$. Alors β est algébrique sur \mathbb{K} , donc est algébrique sur \mathbb{F} car $\mathbb{K} \subset \mathbb{F}$. Ceci montre que $\mathbb{F} \subset \mathbb{E}$ est une extension algébrique.

Supposons maintenant que $\mathbb{K} \subset \mathbb{F}$ et $\mathbb{F} \subset \mathbb{E}$ sont des extensions algébriques. Soit $\beta \in \mathbb{E}$. Il existe un polynôme non nul $f \in \mathbb{F}[X]$ tel que $f(\beta) = 0$. On pose

$$f = a_0 + a_1X + \dots + a_nX^n.$$

Comme $a_0, \dots, a_n \in \mathbb{F}$, ils sont algébriques sur \mathbb{K} , donc, par la proposition 7.9, l'extension $\mathbb{K} \subset \mathbb{K}(a_0, a_1, \dots, a_n)$ est de degré fini. Par ailleurs, comme $f(\beta) = 0$, β est algébrique sur $\mathbb{K}(a_0, a_1, \dots, a_n)$, donc, par la proposition 7.9, $\mathbb{K}(a_0, a_1, \dots, a_n) \subset \mathbb{K}(a_0, a_1, \dots, a_n, \beta)$ est une extension de degré fini. Par la proposition 7.11(1) on en déduit que $\mathbb{K} \subset \mathbb{K}(a_0, a_1, \dots, a_n, \beta)$ est une extension de degré fini donc, par la proposition 7.1, c'est une extension algébrique. En particulier, β est algébrique sur \mathbb{K} . Ceci montre que $\mathbb{K} \subset \mathbb{E}$ est une extension algébrique.

Démonstration de (2). Soient $\mathbb{K}, \mathbb{F}_1, \mathbb{F}_2, \mathbb{E}$ quatre corps tels que $\mathbb{K} \subset \mathbb{F}_1 \subset \mathbb{E}$, $\mathbb{K} \subset \mathbb{F}_2 \subset \mathbb{E}$ et $\mathbb{K} \subset \mathbb{F}_2$ est une extension algébrique. Soit $\beta \in \mathbb{F}_1\mathbb{F}_2$. Par le lemme 7.10 il existe un nombre fini d'éléments $\alpha_1, \dots, \alpha_n \in \mathbb{F}_2$ tels que $\beta \in \mathbb{F}_1(\alpha_1, \dots, \alpha_n)$. Les éléments $\alpha_1, \dots, \alpha_n$ sont algébriques sur \mathbb{K} donc sont algébriques sur \mathbb{F}_1 , donc, par la

proposition 7.9, l'extension $\mathbb{F}_1 \subset \mathbb{F}_1(\alpha_1, \dots, \alpha_n)$ est de degré fini donc algébrique. En particulier, β est algébrique sur \mathbb{F}_1 . Ceci montre que l'extension $\mathbb{F}_1 \subset \mathbb{F}_1\mathbb{F}_2$ est algébrique.

Démonstration de (3). Soient $\mathbb{K}, \mathbb{F}_1, \mathbb{F}_2, \mathbb{E}$ quatre corps tels que $\mathbb{K} \subset \mathbb{F}_1 \subset \mathbb{E}$, $\mathbb{K} \subset \mathbb{F}_2 \subset \mathbb{E}$, et les extensions $\mathbb{K} \subset \mathbb{F}_1$ et $\mathbb{K} \subset \mathbb{F}_2$ sont algébriques. Par (2) $\mathbb{F}_1 \subset \mathbb{F}_1\mathbb{F}_2$ est une extension algébrique, puis, par (1), l'extension $\mathbb{K} \subset \mathbb{F}_1\mathbb{F}_2$ est algébrique. \square

8 Clôture algébrique

Définition. Soient $\mathbb{F} \subset \mathbb{E}_1$ une extension de corps, \mathbb{E}_2 un autre corps et $\sigma : \mathbb{F} \rightarrow \mathbb{E}_2$ un homomorphisme. Un homomorphisme $\tau : \mathbb{E}_1 \rightarrow \mathbb{E}_2$ tel que $\tau|_{\mathbb{F}} = \sigma$ s'appelle un *prolongement* de σ . Si, de plus, $\mathbb{F} \subset \mathbb{E}_2$ et $\sigma = \text{Id}_{\mathbb{F}}$, on dit que τ est un \mathbb{F} -homomorphisme.

Remarque.

- (1) Rappelons que tout homomorphisme $\sigma : \mathbb{F} \rightarrow \mathbb{E}$ entre deux corps est injectif.
- (2) Si $\tau : \mathbb{E}_1 \rightarrow \mathbb{E}_2$ est un \mathbb{F} -homomorphisme, alors τ est une application linéaire d'espaces vectoriels sur \mathbb{F} .

Lemme 8.1. Soit $\mathbb{F} \subset \mathbb{E}$ une extension algébrique. Alors tout \mathbb{F} -endomorphisme $\tau : \mathbb{E} \rightarrow \mathbb{E}$ est un automorphisme.

Démonstration. Soit $\tau : \mathbb{E} \rightarrow \mathbb{E}$ un \mathbb{F} -endomorphisme. Comme souligné précédemment, on sait déjà que τ est injectif, donc reste à démontrer que τ est surjectif.

Soit $\alpha \in \mathbb{E}$. Soit $p \in \mathbb{F}[X]$ le polynôme minimal de α . Notons $\alpha_1, \dots, \alpha_k$ les racines de p qui se trouvent dans \mathbb{E} . On peut en toute généralité supposer que $\alpha = \alpha_1$. Posons

$$p = a_0 + a_1X + \dots + a_dX^d.$$

Pour tout $i \in \{1, \dots, k\}$ on a

$$\begin{aligned} p(\tau(\alpha_i)) &= a_0 + a_1\tau(\alpha_i) + \dots + a_d\tau(\alpha_i)^d = \tau(a_0) + \tau(a_1)\tau(\alpha_i) + \dots + \tau(a_d)\tau(\alpha_i)^d \\ &= \tau(a_0 + a_1\alpha_i + \dots + a_d\alpha_i^d) = \tau(0) = 0, \end{aligned}$$

donc $\tau(\alpha_i) \in \{\alpha_1, \dots, \alpha_k\}$. Par ce qui précède, l'application τ se restreint en une application $\tau : \{\alpha_1, \dots, \alpha_k\} \rightarrow \{\alpha_1, \dots, \alpha_k\}$ injective. Comme $\{\alpha_1, \dots, \alpha_k\}$ est fini, cette application est une bijection. On en déduit qu'il existe $\alpha_i \in \{\alpha_1, \dots, \alpha_k\}$ tel que $\tau(\alpha_i) = \alpha_1 = \alpha$. Ceci montre que τ est surjectif. \square

Notation. Soient $\mathbb{F}_1, \mathbb{F}_2, \mathbb{E}$ trois corps tels que $\mathbb{F}_1 \subset \mathbb{E}$ et $\mathbb{F}_2 \subset \mathbb{E}$. On note $\mathbb{F}_1[\mathbb{F}_2] = \mathbb{F}_2[\mathbb{F}_1]$ le sous-anneau de \mathbb{E} engendré par $\mathbb{F}_1 \cup \mathbb{F}_2$.

Lemme 8.2. Soient $\mathbb{F}_1, \mathbb{F}_2, \mathbb{E}$ trois corps tels que $\mathbb{F}_1 \subset \mathbb{E}$ et $\mathbb{F}_2 \subset \mathbb{E}$.

(1) $\mathbb{F}_1[\mathbb{F}_2]$ est formé des éléments de la forme

$$a_1b_1 + \cdots + a_nb_n,$$

avec $n \in \mathbb{N}$, $a_1, \dots, a_n \in \mathbb{F}_1$ et $b_1, \dots, b_n \in \mathbb{F}_2$.

(2) $\mathbb{F}_1\mathbb{F}_2$ est le corps des fractions de $\mathbb{F}_1[\mathbb{F}_2]$.

Démonstration. Exercice. □

Lemme 8.3. Soient $\mathbb{F}_1, \mathbb{F}_2, \mathbb{E}_1, \mathbb{E}_2$ quatre corps tels que $\mathbb{F}_1 \subset \mathbb{E}_1$ et $\mathbb{F}_2 \subset \mathbb{E}_1$ et $\tau : \mathbb{E}_1 \rightarrow \mathbb{E}_2$ un homomorphisme. Alors

$$\tau(\mathbb{F}_1\mathbb{F}_2) = \tau(\mathbb{F}_1)\tau(\mathbb{F}_2).$$

Démonstration. Soit $\alpha \in \mathbb{F}_1\mathbb{F}_2$. Par le lemme 8.2, il existe $n, m \in \mathbb{N}$, $a_1, \dots, a_n, a'_1, \dots, a'_m \in \mathbb{F}_1$ et $b_1, \dots, b_n, b'_1, \dots, b'_m \in \mathbb{F}_2$ tels que

$$\alpha = \frac{a_1b_1 + \cdots + a_nb_n}{a'_1b'_1 + \cdots + a'_mb'_m}.$$

Alors

$$\tau(\alpha) = \frac{\tau(a_1)\tau(b_1) + \cdots + \tau(a_n)\tau(b_n)}{\tau(a'_1)\tau(b'_1) + \cdots + \tau(a'_m)\tau(b'_m)} \in \tau(\mathbb{F}_1)\tau(\mathbb{F}_2).$$

Ceci montre que $\tau(\mathbb{F}_1\mathbb{F}_2) \subset \tau(\mathbb{F}_1)\tau(\mathbb{F}_2)$. Par ailleurs, $\tau(\mathbb{F}_1\mathbb{F}_2)$ est un sous-corps de \mathbb{E}_2 contenant $\tau(\mathbb{F}_1)$ et $\tau(\mathbb{F}_2)$, donc $\tau(\mathbb{F}_1)\tau(\mathbb{F}_2) \subset \tau(\mathbb{F}_1\mathbb{F}_2)$. On en conclue que $\tau(\mathbb{F}_1\mathbb{F}_2) = \tau(\mathbb{F}_1)\tau(\mathbb{F}_2)$. □

Lemme 8.4. Soient \mathbb{F} un corps et $f \in \mathbb{F}[X]$ un polynôme non constant. Il existe une extension $\mathbb{F} \subset \mathbb{E}$ telle que \mathbb{E} contienne une racine de f .

Démonstration. Soit p un facteur premier de f . Posons $\mathcal{M} = (p)$. Comme p est premier (et $\mathbb{F}[X]$ est un anneau principal), l'idéal \mathcal{M} est maximal, donc $\mathbb{E} = \mathbb{F}[X]/\mathcal{M}$ est un corps. Pour tout $h \in \mathbb{F}[X]$ on note $[h]$ la classe de h dans $\mathbb{F}[X]/\mathcal{M} = \mathbb{E}$. On peut supposer \mathbb{F} inclus dans \mathbb{E} via l'homomorphisme injectif

$$\begin{aligned} \mathbb{F} &\rightarrow \mathbb{E}, \\ a &\mapsto [a]. \end{aligned}$$

Par ailleurs, si $\alpha = [X] \in \mathbb{E}$, alors

$$p(\alpha) = p([X]) = [p(X)] = 0. \quad \square$$

Corollaire 8.5. Soient \mathbb{F} un corps et $f_1, \dots, f_n \in \mathbb{F}[X]$ un nombre fini de polynômes non constants. Il existe une extension $\mathbb{F} \subset \mathbb{E}$ telle que \mathbb{E} contienne une racine de f_i pour tout $i \in \{1, \dots, n\}$.

Démonstration. On raisonne par récurrence sur n . Le cas $n = 1$ est couvert par le lemme 8.4. On suppose que $n \geq 2$ plus l'hypothèse de récurrence. Par récurrence, il existe une extension $\mathbb{F} \subset \mathbb{E}'$ telle que \mathbb{E}' contienne une racine de f_i pour tout $i \in \{1, \dots, n-1\}$. En considérant f_n comme un élément de $\mathbb{E}'[X]$ et en appliquant de nouveau le lemme 8.4, on en déduit qu'il existe une extension $\mathbb{E}' \subset \mathbb{E}$ telle que \mathbb{E} contienne une racine de f_n . Alors \mathbb{E} contient une racine de f_i pour tout $i \in \{1, \dots, n\}$. \square

Définition (Rappel). On dit qu'un corps \mathbb{K} est *algébriquement clos* si tout polynôme non constant à coefficients dans \mathbb{K} a une racine dans \mathbb{K} .

Lemme 8.6. Soient \mathbb{F} un corps algébriquement clos et $\mathbb{F} \subset \mathbb{E}$ une extension algébrique. Alors $\mathbb{F} = \mathbb{E}$.

Démonstration. Soit $\alpha \in \mathbb{E}$. Soit $p \in \mathbb{F}[X]$ le polynôme minimal de α . Comme \mathbb{F} est algébriquement clos, p est de degré 1 (voir le lemme 1.17), donc est de la forme $p = aX + b$ avec $a, b \in \mathbb{F}$, $a \neq 0$. D'où

$$p(\alpha) = a\alpha + b = 0 \quad \Rightarrow \quad \alpha = \frac{-b}{a} \in \mathbb{F}. \quad \square$$

Définition (Rappel). Soit E un ensemble muni d'une relation d'ordre \leq . On dit que E est *inductif* si $E \neq \emptyset$ et si toute chaîne de E admet un majorant.

Axiome (Lemme de Zorn). Soit E un ensemble inductif. Alors E admet un élément maximal.

Lemme 8.7. Soient A un anneau commutatif et I un idéal propre de A . Il existe un idéal maximal \mathcal{M} de A tel que $I \subset \mathcal{M} \subset A$.

Démonstration. Exercice. \square

Proposition 8.8. Soit \mathbb{F} un corps. Il existe une extension $\mathbb{F} \subset \mathbb{E}$ telle que tout polynôme non constant $f \in \mathbb{F}[X]$ contient une racine dans \mathbb{E} .

Démonstration. Soit

$$\mathcal{S} = \{X_f ; f \in \mathbb{F}[X] \text{ et } \deg f \geq 1\}$$

un ensemble abstrait en bijection avec les polynômes non constants de $\mathbb{F}[X]$. On considère l'anneau $\mathbb{F}[\mathcal{S}]$ des polynômes en \mathcal{S} . Si $P \in \mathbb{F}[\mathcal{S}]$, il existe un nombre fini X_{f_1}, \dots, X_{f_n} d'éléments de \mathcal{S} tels que

$$P = P(X_{f_1}, \dots, X_{f_n}) \in \mathbb{F}[X_{f_1}, \dots, X_{f_n}] \subset \mathbb{F}[\mathcal{S}].$$

Soit

$$\mathcal{I} = \{f(X_f) ; f \in \mathbb{F}[X] \text{ et } \deg f \geq 1\} \subset \mathbb{F}[\mathcal{S}].$$

Assertion. \mathcal{I} est un idéal propre de $\mathbb{F}[\mathcal{S}]$.

Preuve. On raisonne par l'absurde et on suppose que $\mathcal{I} = \mathbb{F}[\mathcal{S}]$, en particulier que $1 \in \mathcal{I}$. Il existe $n \in \mathbb{N}$, $f_1, \dots, f_n \in \mathbb{F}[X]$ non constants, et $P_1, \dots, P_n \in \mathbb{F}[\mathcal{S}]$ tels que

$$(*) \quad 1 = P_1 f_1(X_{f_1}) + \dots + P_n f_n(X_{f_n}).$$

Par le corollaire 8.5, il existe une extension $\mathbb{F} \subset \mathbb{E}'$ qui contient une racine α_i de f_i pour tout $i \in \{1, \dots, n\}$. Soit $\psi : \mathbb{F}[\mathcal{S}] \rightarrow \mathbb{E}'$ l'homomorphisme défini par :

$$\begin{aligned} \psi|_{\mathbb{F}} &= \text{Id}_{\mathbb{F}}, \\ \psi(X_{f_i}) &= \alpha_i \quad \text{pour } i \in \{1, \dots, n\}, \\ \psi(X_f) &= 0 \quad \text{si } f \notin \{f_1, \dots, f_n\}. \end{aligned}$$

En appliquant ψ à $(*)$ on obtient

$$\begin{aligned} 1 &= \psi(P_1) \psi(f_1(X_{f_1})) + \dots + \psi(P_n) \psi(f_n(X_{f_n})) \\ &= \psi(P_1) f_1(\alpha_1) + \dots + \psi(P_n) f_n(\alpha_n) = 0. \end{aligned}$$

Ceci est une contradiction, donc $1 \notin \mathcal{I}$ et donc $\mathcal{I} \neq \mathbb{F}[\mathcal{S}]$.

Fin de la démonstration. Soit \mathcal{M} un idéal maximal de $\mathbb{F}[\mathcal{S}]$ qui contient \mathcal{I} . Posons $\mathbb{E} = \mathbb{F}[\mathcal{S}]/\mathcal{M}$. Comme \mathcal{M} est un idéal maximal, \mathbb{E} est un corps. Soit $\varphi : \mathbb{F} \rightarrow \mathbb{E}$ l'homomorphisme naturel. Comme \mathbb{F} est un corps, cet homomorphisme est injectif, donc on peut supposer que \mathbb{F} est un sous-corps de \mathbb{E} en l'identifiant à $\varphi(\mathbb{F})$.

Pour $P \in \mathbb{F}[\mathcal{S}]$ on note $[P]$ l'élément de $\mathbb{E} = \mathbb{F}[\mathcal{S}]/\mathcal{M}$ représenté par P . Si $f \in \mathbb{F}[X]$ est un polynôme non constant, on pose

$$\alpha_f = [X_f] \in \mathbb{E}.$$

Alors, pour $f \in \mathbb{F}[X]$ non constant, on a

$$f(\alpha_f) = [f(X_f)] = 0,$$

car $f(X_f) \in \mathcal{I} \subset \mathcal{M}$. Ceci montre que tout polynôme non constant de $\mathbb{F}[X]$ admet une racine dans \mathbb{E} . \square

Théorème 8.9. *Soit \mathbb{F} un corps. Il existe une extension $\mathbb{F} \subset \mathbb{E}$ telle que \mathbb{E} soit algébriquement clos.*

Démonstration. On définit une suite de corps \mathbb{E}_n , $n \in \mathbb{N}$, par récurrence sur n comme suit. On pose $\mathbb{E}_0 = \mathbb{F}$. Supposons que \mathbb{E}_n soit défini. Alors \mathbb{E}_{n+1} est un corps contenant \mathbb{E}_n tel que tout polynôme non constant $f \in \mathbb{E}_n[X]$ a une racine dans \mathbb{E}_{n+1} . La proposition 8.8 garantit qu'une telle extension $\mathbb{E}_n \subset \mathbb{E}_{n+1}$ existe. On a une chaîne

$$\mathbb{F} = \mathbb{E}_0 \subset \mathbb{E}_1 \subset \dots \subset \mathbb{E}_n \subset \mathbb{E}_{n+1} \subset \dots$$

On pose

$$\mathbb{E} = \bigcup_{n=0}^{\infty} \mathbb{E}_n.$$

On définit des opérations $+$ et \cdot dans \mathbb{E} comme suit. Soient $x, y \in \mathbb{E}$. Par définition, il existe $n_1, n_2 \in \mathbb{N}$ tels que $x \in \mathbb{E}_{n_1}$ et $y \in \mathbb{E}_{n_2}$. Posons $n = \max\{n_1, n_2\}$. On a $x, y \in \mathbb{E}_n$. Alors $x + y$ est la somme de x et y dans \mathbb{E}_n et $x \cdot y$ est le produit de x et y dans \mathbb{E}_n . On vérifie facilement que ces opérations sont bien définies et que \mathbb{E} muni de ces opérations est un corps. Il est évident qu'il contient $\mathbb{E}_0 = \mathbb{F}$. Reste à montrer qu'il est algébriquement clos.

Soit

$$f = a_0 + a_1X + \cdots + a_dX^d$$

un polynôme non constant à coefficients dans \mathbb{E} . Pour tout $i \in \{1, \dots, d\}$ il existe $n_i \in \mathbb{N}$ tel que $a_i \in \mathbb{E}_{n_i}$. Posons $n = \max\{n_1, \dots, n_d\}$. Alors $a_1, \dots, a_d \in \mathbb{E}_n$, donc $f \in \mathbb{E}_n[X]$. Par construction il existe $\alpha \in \mathbb{E}_{n+1}$ tel que $f(\alpha) = 0$. Ceci montre que \mathbb{E} est algébriquement clos. \square

Théorème 8.10. *Soit \mathbb{F} un corps. Il existe une extension algébrique $\mathbb{F} \subset \mathbb{E}$ telle que \mathbb{E} est algébriquement clos.*

Définition. Soit \mathbb{F} un corps. Si $\mathbb{F} \subset \mathbb{E}$ est une extension algébrique telle que \mathbb{E} est algébriquement clos, on dit que \mathbb{E} est une *clôture algébrique* de \mathbb{F} .

Démonstration. Par le théorème 8.9 il existe une extension $\mathbb{F} \subset \hat{\mathbb{E}}$ telle que $\hat{\mathbb{E}}$ est algébriquement clos. Posons

$$\mathbb{E} = \{\alpha \in \hat{\mathbb{E}} ; \alpha \text{ est algébrique sur } \mathbb{F}\}.$$

Il est clair que $0, 1 \in \mathbb{E}$. Soient $\alpha, \beta \in \mathbb{E}$. L'extension $\mathbb{F} \subset \mathbb{F}(\alpha, \beta)$ est de degré fini, donc algébrique, donc $\alpha - \beta$ est algébrique sur \mathbb{F} , et, si $\alpha \neq 0$ et $\beta \neq 0$, alors $\alpha\beta^{-1}$ est algébrique sur \mathbb{F} . Ceci montre que \mathbb{E} est un sous-corps de $\hat{\mathbb{E}}$. De plus, par construction, l'extension $\mathbb{F} \subset \mathbb{E}$ est algébrique. Reste à montrer que \mathbb{E} est algébriquement clos.

Soit $f \in \mathbb{E}[X]$ non constant. Comme $\hat{\mathbb{E}}$ est algébriquement clos, f a une racine dans $\hat{\mathbb{E}}$, α . Les extensions $\mathbb{F} \subset \mathbb{E}$ et $\mathbb{E} \subset \mathbb{E}(\alpha)$ sont algébriques, donc l'extension $\mathbb{F} \subset \mathbb{E}(\alpha)$ est algébrique (voir proposition 7.12), donc α est algébrique sur \mathbb{F} , c'est-à-dire $\alpha \in \mathbb{E}$. Ceci montre que \mathbb{E} est algébriquement clos. \square

Proposition 8.11. *Soient $\mathbb{F}, \mathbb{E}, \mathbb{L}$ trois corps tels que $\mathbb{F} \subset \mathbb{E}$ et \mathbb{L} est algébriquement clos, $\sigma : \mathbb{F} \rightarrow \mathbb{L}$ un homomorphisme, et $\alpha \in \mathbb{E}$ un élément algébrique sur \mathbb{F} . Soit $p = a_0 + a_1X + \cdots + a_dX^d$ le polynôme minimal de α ,*

$$\sigma(p) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_d)X^d,$$

et β_1, \dots, β_m les racines de $\sigma(p)$ dans \mathbb{L} .

(1) Pour tout $i \in \{1, \dots, m\}$ il existe une extension $\varphi_i : \mathbb{F}(\alpha) \rightarrow \mathbb{L}$ de σ qui envoie α sur β_i .

(2) Si $\varphi : \mathbb{F}(\alpha) \rightarrow \mathbb{L}$ est une extension de σ , alors il existe $i \in \{1, \dots, m\}$ tel que $\varphi = \varphi_i$.

Remarque. On a $\varphi_i \neq \varphi_j$ pour $i, j \in \{1, \dots, m\}$, $i \neq j$, car

$$\varphi_i(\alpha) = \beta_i \neq \beta_j = \varphi_j(\alpha).$$

Démonstration. Rappelons que l'on a l'isomorphisme

$$\mu : \mathbb{F}[X]/(p) \rightarrow \mathbb{F}(\alpha)$$

qui envoie $[X]$ sur α (voir proposition 7.5 (2)). Pour $i \in \{1, \dots, m\}$ on définit l'homomorphisme $\hat{\psi}_i : \mathbb{F}[X] \rightarrow \mathbb{L}$ en posant

$$\hat{\psi}_i(b_0 + b_1X + \dots + b_nX^n) = \sigma(b_0) + \sigma(b_1)\beta_i + \dots + \sigma(b_n)\beta_i^n.$$

On a $\hat{\psi}_i(p) = \sigma(p)(\beta_i) = 0$, donc $\hat{\psi}_i$ induit un homomorphisme $\psi_i : \mathbb{F}[X]/(p) \rightarrow \mathbb{L}$. On pose

$$\varphi_i = \psi_i \circ \mu^{-1} : \mathbb{F}(\alpha) \rightarrow \mathbb{L}.$$

Il est clair que φ_i est une extension de σ et $\varphi_i(\alpha) = \beta_i$.

Soit $\varphi : \mathbb{F}(\alpha) \rightarrow \mathbb{L}$ une extension de σ . Posons

$$\psi = \varphi \circ \mu : \mathbb{F}[X]/(p) \rightarrow \mathbb{L}, \quad \hat{\psi} = \psi \circ \pi : \mathbb{F}[X] \rightarrow \mathbb{L},$$

où $\pi : \mathbb{F}[X] \rightarrow \mathbb{F}[X]/(p)$ est la projection naturelle. Soit $\beta = \hat{\psi}(X)$. On a $0 = \hat{\psi}(p) = \sigma(p)(\beta)$, donc β est une racine de p , c'est-à-dire qu'il existe $i \in \{1, \dots, m\}$ tel que $\beta = \beta_i$. On a alors $\hat{\psi} = \hat{\psi}_i$, $\psi = \psi_i$ et $\varphi = \varphi_i$. \square

Théorème 8.12. Soient \mathbb{F} un corps, et $\mathbb{F} \subset \mathbb{E}$, $\mathbb{F} \subset \mathbb{L}$ deux extensions algébriques telles que \mathbb{L} est algébriquement clos. Alors il existe un \mathbb{F} -homomorphisme $\sigma : \mathbb{E} \rightarrow \mathbb{L}$.

Démonstration. Soit \mathcal{S} l'ensemble des couples (\mathbb{K}, τ) , où \mathbb{K} est un sous-corps de \mathbb{E} contenant \mathbb{F} (i.e. $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$) et $\tau : \mathbb{K} \rightarrow \mathbb{L}$ est un \mathbb{F} -homomorphisme. Remarquons que $\mathcal{S} \neq \emptyset$ car $(\mathbb{F}, \text{Id}_{\mathbb{F}}) \in \mathcal{S}$. On définit une relation d'ordre \leq sur \mathcal{S} par :

$$(\mathbb{K}_1, \tau_1) \leq (\mathbb{K}_2, \tau_2) \text{ si } \mathbb{K}_1 \subset \mathbb{K}_2 \text{ et } \tau_2|_{\mathbb{K}_1} = \tau_1.$$

Soit $\mathcal{C} = \{(\mathbb{K}_i, \tau_i)\}_{i \in I}$ un chaîne non vide dans \mathcal{S} . Posons

$$\mathbb{K} = \bigcup_{i \in I} \mathbb{K}_i.$$

Montrons que \mathbb{K} est un sous-corps de \mathbb{E} . Soient $\alpha, \beta \in \mathbb{K}$. Il existe $i, j \in I$ tels que $\alpha \in \mathbb{K}_i$ et $\beta \in \mathbb{K}_j$. On peut en toute généralité supposer que $(\mathbb{K}_i, \tau_i) \leq (\mathbb{K}_j, \tau_j)$. On alors $\alpha, \beta \in \mathbb{K}_j$, donc $\alpha - \beta \in \mathbb{K}_j \subset \mathbb{K}$ et, si $\alpha, \beta \neq 0$, $\alpha\beta^{-1} \in \mathbb{K}_j \subset \mathbb{K}$.

On définit $\tau : \mathbb{K} \rightarrow \mathbb{L}$ comme suit. Soit $\alpha \in \mathbb{K}$. Soit $i \in I$ tel que $\alpha \in \mathbb{K}_i$. On pose

$$\tau(\alpha) = \tau_i(\alpha).$$

On vérifie facilement que τ est bien défini et est un homomorphisme. Il est clair que (\mathbb{K}, τ) est un majorant de \mathcal{C} .

Par le lemme de Zorn, \mathcal{S} a un élément maximal, (\mathbb{K}, τ) . Montrons par l'absurde que $\mathbb{K} = \mathbb{E}$. On suppose que $\mathbb{K} \neq \mathbb{E}$. On choisit $\alpha \in \mathbb{E} \setminus \mathbb{K}$. Comme α est algébrique sur \mathbb{K} , par la proposition 8.11, τ admet une extension $\tilde{\tau} : \mathbb{K}(\alpha) \rightarrow \mathbb{L}$. On a $(\mathbb{K}(\alpha), \tilde{\tau}) \in \mathcal{S}$ et $(\mathbb{K}, \tau) \prec (\mathbb{K}(\alpha), \tilde{\tau})$ ce qui contredit la maximalité de (\mathbb{K}, τ) . D'où $\mathbb{K} = \mathbb{E}$ et $\tau : \mathbb{E} \rightarrow \mathbb{L}$ est un \mathbb{F} -homomorphisme. \square

Théorème 8.13. *Soient \mathbb{F} un corps et $\mathbb{E}_1, \mathbb{E}_2$ deux clôtures algébriques de \mathbb{F} . Alors il existe un \mathbb{F} -isomorphisme $\tau : \mathbb{E}_1 \rightarrow \mathbb{E}_2$.*

Démonstration. Par le théorème 8.12 il existe un \mathbb{F} -homomorphisme $\tau : \mathbb{E}_1 \rightarrow \mathbb{E}_2$. On sait que τ est injectif car \mathbb{E}_1 est un corps, donc il reste à montrer que τ est surjectif. Comme \mathbb{E}_1 est algébriquement clos, $\tau(\mathbb{E}_1)$ est aussi algébriquement clos. Par ailleurs $\mathbb{F} \subset \mathbb{E}_2$ est une extension algébrique et $\mathbb{F} \subset \tau(\mathbb{E}_1) \subset \mathbb{E}_2$, donc $\tau(\mathbb{E}_1) \subset \mathbb{E}_2$ est une extension algébrique. Par le lemme 8.6 on en conclue que $\tau(\mathbb{E}_1) = \mathbb{E}_2$. \square

9 Corps de décomposition et extensions normales

Définition. Soient \mathbb{F} un corps, $\mathbb{K} \supset \mathbb{F}$ une extension, et $f \in \mathbb{F}[X]$ un polynôme non constant. On dit que \mathbb{K} est un *corps de décomposition* de f s'il existe $\alpha_1, \dots, \alpha_l \in \mathbb{K}$ et $c \in \mathbb{F}$ tels que

$$f = c(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_l),$$

et $\mathbb{K} = \mathbb{F}(\alpha_1, \dots, \alpha_l)$.

Remarque. Dans la définition antérieure c doit être le coefficient dominant de f .

Théorème 9.1. *Soient \mathbb{F} un corps et $f \in \mathbb{F}[X]$ un polynôme non constant.*

- (1) *Soient $\mathbb{K}_1, \mathbb{K}_2$ deux corps de décomposition de f . Alors il existe un \mathbb{F} -isomorphisme $\sigma : \mathbb{K}_1 \rightarrow \mathbb{K}_2$.*
- (2) *Soit \mathbb{L} une clôture algébrique de \mathbb{F} . Il existe un unique sous-corps $\mathbb{K} \subset \mathbb{L}$ tel que $\mathbb{F} \subset \mathbb{K}$ et \mathbb{K} est un corps de décomposition de f .*

Démonstration. Notons c le coefficient dominant de f . Soient $\alpha_1, \dots, \alpha_l \in \mathbb{K}_1$ tels que

$$f = c(X - \alpha_1) \cdots (X - \alpha_l)$$

et $\mathbb{K}_1 = \mathbb{F}(\alpha_1, \dots, \alpha_l)$, et $\beta_1, \dots, \beta_l \in \mathbb{K}_2$ tels que

$$f = c(X - \beta_1) \cdots (X - \beta_l)$$

et $\mathbb{K}_2 = \mathbb{F}(\beta_1, \dots, \beta_l)$. Soit \mathbb{L}_2 une clôture algébrique de \mathbb{K}_2 . Comme $\mathbb{F} \subset \mathbb{K}_2$ et $\mathbb{K}_2 \subset \mathbb{L}_2$ sont des extensions algébriques, $\mathbb{F} \subset \mathbb{L}_2$ est une extension algébrique. Comme, de plus, \mathbb{L}_2 est algébriquement clos, \mathbb{L}_2 est une clôture algébrique de \mathbb{F} . Le fait que $\mathbb{F} \subset \mathbb{K}_1$ est une extension algébrique, par le théorème 8.12, implique qu'il existe un \mathbb{F} -homomorphisme $\sigma : \mathbb{K}_1 \rightarrow \mathbb{L}_2$.

Notons $\hat{\sigma} : \mathbb{K}_1[X] \rightarrow \mathbb{L}_2[X]$ l'homomorphisme induit par σ . On observe que

$$f = \sigma(f) = c(X - \sigma(\alpha_1)) \cdots (X - \sigma(\alpha_l))$$

donc $\sigma(\alpha_1), \dots, \sigma(\alpha_l)$ sont les racines de f dans \mathbb{L}_2 , donc $\{\sigma(\alpha_1), \dots, \sigma(\alpha_l)\} = \{\beta_1, \dots, \beta_l\}$. Il en résulte qu'il existe une permutation $\chi \in \mathfrak{S}_l$ telle que $\beta_{\chi(i)} = \sigma(\alpha_i)$ pour tout i , d'où $\sigma(\mathbb{K}_1) = \mathbb{F}(\sigma(\alpha_1), \dots, \sigma(\alpha_l)) = \mathbb{F}(\beta_1, \dots, \beta_l) = \mathbb{K}_2$.

Maintenant on démontre la seconde partie du théorème. On suppose que \mathbb{L} est une clôture algébrique de \mathbb{F} . Soient $\alpha_1, \dots, \alpha_l$ les racines de f dans \mathbb{L} . On a

$$f = c(X - \alpha_1) \cdots (X - \alpha_l).$$

Posons $\mathbb{K} = \mathbb{F}(\alpha_1, \dots, \alpha_l)$. Alors \mathbb{K} est un corps de décomposition de f inclus dans \mathbb{L} . Il est clairement le seul corps de décomposition de f inclus dans \mathbb{L} . \square

Corollaire 9.2. *Soient \mathbb{F} un corps et $f \in \mathbb{F}[X]$ un polynôme non constant. Alors il existe un corps de décomposition de f .*

Définition. Soient $\mathbb{F} \subset \mathbb{K}$ une extension de corps et $\mathcal{F} = \{f_i\}_{i \in I}$ une famille de polynômes dans $\mathbb{F}[X]$. On dit que \mathbb{K} est un *corps de décomposition* de \mathcal{F} si

- (a) f_i se décompose en facteurs linéaires dans $\mathbb{K}[X]$ pour tout $i \in I$;
- (b) \mathbb{K} est l'extension de \mathbb{F} engendré par toutes les racines de tous les f_i .

Théorème 9.3. *Soient \mathbb{F} un corps et $\mathcal{F} = \{f_i\}_{i \in I}$ une famille de polynômes dans $\mathbb{F}[X]$.*

- (1) *Soient $\mathbb{K}_1, \mathbb{K}_2$ deux corps de décomposition de \mathcal{F} . Alors il existe un \mathbb{F} -isomorphisme $\sigma : \mathbb{K}_1 \rightarrow \mathbb{K}_2$.*
- (2) *Soit \mathbb{L} une clôture algébrique de \mathbb{F} . Il existe un unique sous-corps $\mathbb{K} \subset \mathbb{L}$ tel que $\mathbb{F} \subset \mathbb{K}$ et \mathbb{K} est un corps de décomposition de \mathcal{F} .*

Démonstration. Exercice. □

Corollaire 9.4. Soient \mathbb{F} un corps et $\mathcal{F} = \{f_i\}_{i \in I}$ une famille de polynômes dans $\mathbb{F}[X]$. Alors il existe un corps de décomposition de \mathcal{F} .

Théorème 9.5. Soient \mathbb{F} un corps, \mathbb{L} une clôture algébrique de \mathbb{F} , et \mathbb{K} un corps tel que $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$. Alors les 3 conditions suivantes sont équivalentes.

- (a) Tout \mathbb{F} -homomorphisme $\sigma : \mathbb{K} \rightarrow \mathbb{L}$ induit un \mathbb{F} -automorphisme $\sigma : \mathbb{K} \rightarrow \mathbb{K}$.
- (b) \mathbb{K} est un corps de décomposition pour une famille $\mathcal{F} = \{f_i\}_{i \in I}$ de polynômes de $\mathbb{F}[X]$.
- (c) Tout polynôme irréductible de $\mathbb{F}[X]$ ayant une racine dans \mathbb{K} se décompose en facteurs linéaires dans $\mathbb{K}[X]$.

Démonstration. (a) \Rightarrow (c). On suppose que tout \mathbb{F} -homomorphisme $\sigma : \mathbb{K} \rightarrow \mathbb{L}$ induit un \mathbb{F} -isomorphisme $\sigma : \mathbb{K} \rightarrow \mathbb{K}$. Soit $p \in \mathbb{F}[X]$ un polynôme irréductible ayant une racine $\alpha \in \mathbb{K}$. Soient $\alpha_1, \dots, \alpha_d$ les racines de p qui sont dans \mathbb{L} . On a

$$p = c(X - \alpha_1) \cdots (X - \alpha_d),$$

où c est le coefficient dominant de p .

Par la proposition 8.11, pour tout $i \in \{1, \dots, d\}$ il existe un \mathbb{F} -homomorphisme $\varphi_i : \mathbb{F}(\alpha) \rightarrow \mathbb{L}$ qui envoie α sur α_i . Par le théorème 8.12 (il faut le modifier un peu) φ_i s'étend en un \mathbb{F} -homomorphisme $\hat{\varphi}_i : \mathbb{K} \rightarrow \mathbb{L}$. Par hypothèse, l'image de $\hat{\varphi}_i$ est \mathbb{K} , en particulier $\alpha_i = \hat{\varphi}_i(\alpha) \in \mathbb{K}$. Ceci montre que p se décompose en facteurs linéaires dans $\mathbb{K}[X]$.

(c) \Rightarrow (b). Soit \mathcal{F} l'ensemble des polynômes irréductibles $p \in \mathbb{F}[X]$ ayant une racine dans \mathbb{K} . Montrons que \mathbb{K} est le corps de décomposition de \mathcal{F} . Soit $p \in \mathcal{F}$. Alors p se décompose en facteurs linéaires par définition. Soit $\alpha \in \mathbb{K} \setminus \mathbb{F}$. Soit p le polynôme minimal de α dans $\mathbb{F}[X]$. Alors p est un polynôme irréductible dans $\mathbb{F}[X]$ qui a au moins une racine dans \mathbb{K} , donc $p \in \mathcal{F}$. Ceci montre que \mathbb{K} est l'extension de \mathbb{F} engendrée par les racines des éléments de \mathcal{F} .

(b) \Rightarrow (a). Supposons que \mathbb{K} est le corps de décomposition d'une famille $\mathcal{F} = \{f_i\}_{i \in I}$ de polynômes dans $\mathbb{F}[X]$. Soit $\sigma : \mathbb{K} \rightarrow \mathbb{L}$ un \mathbb{F} -plongement. Le corps $\sigma(\mathbb{K})$ est aussi un corps de décomposition de \mathcal{F} . L'unicité d'un tel corps implique que $\sigma(\mathbb{K}) = \mathbb{K}$, donc σ induit un \mathbb{F} -automorphisme $\sigma : \mathbb{K} \rightarrow \mathbb{K}$. □

Définition. Si une extension $\mathbb{F} \subset \mathbb{K}$ vérifie les trois propriétés équivalentes du théorème 9.5, on dit que $\mathbb{F} \subset \mathbb{K}$ est une *extension normale* ou *quasi-galoisienne*.

Théorème 9.6.

- (1) Soient $\mathbb{F}, \mathbb{K}, \mathbb{L}$ trois corps tels que $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$. Si l'extension $\mathbb{F} \subset \mathbb{L}$ est normale, alors l'extension $\mathbb{K} \subset \mathbb{L}$ est normale.
- (2) Soient $\mathbb{F}, \mathbb{K}_1, \mathbb{K}_2, \mathbb{L}$ quatre corps tels que $\mathbb{F} \subset \mathbb{K}_1 \subset \mathbb{L}$ et $\mathbb{F} \subset \mathbb{K}_2 \subset \mathbb{L}$. Si $\mathbb{F} \subset \mathbb{K}_1$ et $\mathbb{F} \subset \mathbb{K}_2$ sont deux extensions normales, alors $\mathbb{F} \subset \mathbb{K}_1\mathbb{K}_2$ est une extension normale.
- (3) Soient $\mathbb{F}, \mathbb{K}_1, \mathbb{K}_2, \mathbb{L}$ quatre corps tels que $\mathbb{F} \subset \mathbb{K}_1 \subset \mathbb{L}$ et $\mathbb{F} \subset \mathbb{K}_2 \subset \mathbb{L}$. Si $\mathbb{F} \subset \mathbb{K}_1$ et $\mathbb{F} \subset \mathbb{K}_2$ sont deux extensions normales, alors $\mathbb{F} \subset \mathbb{K}_1 \cap \mathbb{K}_2$ est une extension normale.

Démonstration. On se donne trois corps $\mathbb{F}, \mathbb{K}, \mathbb{L}$ tels que $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$ et on suppose que l'extension $\mathbb{F} \subset \mathbb{L}$ est normale. Soit $\bar{\mathbb{L}}$ une clôture algébrique de \mathbb{L} . Alors $\bar{\mathbb{L}}$ est aussi une clôture algébrique de \mathbb{F} et de \mathbb{K} . Si $\sigma : \mathbb{L} \rightarrow \bar{\mathbb{L}}$ est un \mathbb{K} -plongement, alors $\sigma : \mathbb{L} \rightarrow \bar{\mathbb{L}}$ est un \mathbb{F} -plongement, donc $\sigma(\mathbb{L}) = \mathbb{L}$ car $\mathbb{F} \subset \mathbb{L}$ est une extension normale. Ceci montre que $\mathbb{K} \subset \mathbb{L}$ est une extension normale.

Soient $\mathbb{F}, \mathbb{K}_1, \mathbb{K}_2, \mathbb{L}$ quatre corps tels que $\mathbb{F} \subset \mathbb{K}_1 \subset \mathbb{L}$, $\mathbb{F} \subset \mathbb{K}_2 \subset \mathbb{L}$ et $\mathbb{F} \subset \mathbb{K}_1$, $\mathbb{F} \subset \mathbb{K}_2$ sont des extensions normales. Posons

$$\mathbb{L}^0 = \{\alpha \in \mathbb{L}; \alpha \text{ est algébrique sur } \mathbb{F}\}.$$

Alors \mathbb{L}^0 est un corps, $\mathbb{K}_1, \mathbb{K}_2 \subset \mathbb{L}^0$ car $\mathbb{F} \subset \mathbb{K}_1$ et $\mathbb{F} \subset \mathbb{K}_2$ sont des extensions algébriques, et $\mathbb{K}_1\mathbb{K}_2 \subset \mathbb{L}^0$ par la proposition 7.12. Soit $\bar{\mathbb{L}}$ une clôture algébrique de \mathbb{L}^0 . C'est aussi une clôture algébrique de \mathbb{K}_1 , \mathbb{K}_2 et $\mathbb{K}_1\mathbb{K}_2$. Soit $\sigma : \mathbb{K}_1\mathbb{K}_2 \rightarrow \bar{\mathbb{L}}$ un \mathbb{F} -plongement. On a $\sigma(\mathbb{K}_1\mathbb{K}_2) = \sigma(\mathbb{K}_1)\sigma(\mathbb{K}_2)$ par le lemme 8.3 et $\sigma(\mathbb{K}_1) = \mathbb{K}_1$ et $\sigma(\mathbb{K}_2) = \mathbb{K}_2$ car $\mathbb{F} \subset \mathbb{K}_1$ et $\mathbb{F} \subset \mathbb{K}_2$ sont des extensions normales, donc $\sigma(\mathbb{K}_1\mathbb{K}_2) = \mathbb{K}_1\mathbb{K}_2$. Ceci montre que $\mathbb{F} \subset \mathbb{K}_1\mathbb{K}_2$ est une extension normale.

Soit $\sigma : \mathbb{K}_1 \cap \mathbb{K}_2 \rightarrow \bar{\mathbb{L}}$ un \mathbb{F} -plongement. Alors σ s'étend en un \mathbb{F} -plongement $\tau : \mathbb{L}^0 \rightarrow \bar{\mathbb{L}}$. Comme $\mathbb{F} \subset \mathbb{K}_1$ et $\mathbb{F} \subset \mathbb{K}_2$ sont des extensions normales, on a $\tau(\mathbb{K}_1) = \mathbb{K}_1$ et $\tau(\mathbb{K}_2) = \mathbb{K}_2$, donc

$$\sigma(\mathbb{K}_1 \cap \mathbb{K}_2) = \tau(\mathbb{K}_1 \cap \mathbb{K}_2) = \tau(\mathbb{K}_1) \cap \tau(\mathbb{K}_2) = \mathbb{K}_1 \cap \mathbb{K}_2.$$

Ceci montre que $\mathbb{F} \subset \mathbb{K}_1 \cap \mathbb{K}_2$ est une extension normale. □

10 Corps finis

Théorème 10.1.

- (1) Soient p un nombre premier et n un entier ≥ 1 . Alors il existe un corps \mathbb{F}_q de cardinal q , où $q = p^n$.
- (2) Soit \mathbb{K} un corps fini. Alors il existe un nombre premier p et un entier $n \geq 1$ tels que $\mathbb{K} \simeq \mathbb{F}_q$, où $q = p^n$.

Démonstration. Soit p un nombre premier. Posons $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Alors \mathbb{F}_p est un corps de cardinal p . Soit maintenant n un entier ≥ 1 . Posons $q = p^n$ et notons \mathbb{F}_q le corps de décomposition de $f = X^q - X$ sur \mathbb{F}_p . Soit U l'ensemble des racines de f . On va montrer que $\mathbb{F}_q = U$. Toute les racines de f sont simples (car $f' = 1 \neq 0$), donc on aura $|\mathbb{F}_q| = |U| = \deg f = q$.

Pour montrer que $U = \mathbb{F}_q$, il suffit de montrer que U est un sous-corps de \mathbb{F}_q . Comme U contiendra toutes les racines de f et \mathbb{F}_q est un corps de décomposition de f , cela impliquera que $\mathbb{F}_q = U$.

- $0^q - 0 = 0$, donc $0 \in U$. Par ailleurs, $1^q - 1 = 1 - 1 = 0$, donc $1 \in U$.
- Soit $\alpha \in U$. Si $p = 2$, alors $-\alpha = \alpha$, donc $-\alpha \in U$. Si $p \neq 2$, alors $q = p^n$ est impair, donc

$$(-\alpha)^q - (-\alpha) = -(\alpha^q - \alpha) = 0.$$

Dans les deux cas on a $-\alpha \in U$.

- Soit $\alpha \in U$, $\alpha \neq 0$. Alors

$$\begin{aligned} \alpha^q - \alpha &= \alpha(\alpha^{q-1} - 1) = 0 \\ \Rightarrow \alpha^{q-1} - 1 &= 0 \\ \Rightarrow \alpha^{q-1} &= 1 \\ \Rightarrow (\alpha^{-1})^{q-1} &= 1 \\ \Rightarrow (\alpha^{-1})^q - \alpha^{-1} &= 0 \end{aligned}$$

donc $\alpha^{-1} \in U$.

- Soient $\alpha, \beta \in U$. Alors

$$(\alpha + \beta)^p = \alpha^p + \beta^p \Rightarrow (\alpha + \beta)^q = \alpha^q + \beta^q = \alpha + \beta,$$

donc $\alpha + \beta \in U$. Par ailleurs

$$(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta,$$

donc $\alpha\beta \in U$.

- Soit $a \in \mathbb{F}_p$. Si $a = 0$, alors $a^q = a = 0$. Supposons que $a \neq 0$. Alors a appartient à \mathbb{F}_p^* qui est d'ordre $p - 1$, donc $a^{p-1} = 1$, donc $a^p = a$. Finalement,

$$a^q = (a^p)^{p^{n-1}} = a^{p^{n-1}} = \dots = a,$$

d'où $a \in U$.

Ces points montrent que U est un sous-corps de \mathbb{F}_q contenant \mathbb{F}_p .

Soit \mathbb{K} un corps fini. Rappelons l'homomorphisme caractéristique $\mu : \mathbb{Z} \rightarrow \mathbb{K}$, $1 \mapsto 1_{\mathbb{K}}$. Soit $p\mathbb{Z}$ le noyau de μ . $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à un sous-anneau de \mathbb{K} qui est intègre, donc doit être intègre, donc p est un nombre premier. En identifiant $\mathbb{Z}/p\mathbb{Z}$ à l'image de μ , on peut supposer que $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un sous-corps de \mathbb{K} .

Notons n la dimension de \mathbb{K} vu comme espace vectoriel sur \mathbb{F}_p . Comme \mathbb{K} est isomorphe à $(\mathbb{F}_p)^n$ en tant qu'espace vectoriel sur \mathbb{F}_p , on a $|\mathbb{K}| = p^n$. Posons $q = p^n$. Soit $\alpha \in \mathbb{K}$. Si $\alpha = 0$, alors $\alpha^q - \alpha = 0 - 0 = 0$. Supposons que $\alpha \neq 0$. On a $\alpha \in \mathbb{K}^*$ qui est d'ordre $q - 1$, donc

$$\begin{aligned} \alpha^{q-1} &= 1 \\ \Rightarrow \alpha^{q-1} - 1 &= 0 \\ \Rightarrow \alpha^q - \alpha &= 0 \end{aligned}$$

Donc, tout élément de \mathbb{K} est une racine de $f = X^q - X$, donc $\mathbb{K} \subset \mathbb{F}_q$. Comme, de plus, $|\mathbb{K}| = |\mathbb{F}_q| = q$, on conclut que $\mathbb{K} = \mathbb{F}_q$. \square

Définition. Soient p un nombre premier et n un entier ≥ 1 . Posons $q = p^n$. Alors l'application

$$\begin{aligned} \varphi : \mathbb{F}_q &\rightarrow \mathbb{F}_q \\ \alpha &\mapsto \alpha^p \end{aligned}$$

est un automorphisme appelé *automorphisme de Frobenius*.

Définition. Soit \mathbb{K} un corps. Le *groupe de Galois* de \mathbb{K} est le groupe $\text{Gal}(\mathbb{K})$ de automorphismes de \mathbb{K} . Si $\mathbb{F} \subset \mathbb{K}$ est une extension, on note aussi $\text{Gal}(\mathbb{K}/\mathbb{F})$ le groupe des \mathbb{F} -automorphismes de \mathbb{K} .

Théorème 10.2. Soient p un nombre premier et n, m deux entiers ≥ 1 . Posons $q = p^n$. Alors $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ est un groupe cyclique d'ordre m engendré par φ^n , où $\varphi : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$ est l'automorphisme de Frobenius.

Démonstration. Posons $\psi = \varphi^n$. Pour $\alpha \in \mathbb{F}_q$ on a

$$\psi(\alpha) = \varphi^n(\alpha) = \alpha^{p^n} = \alpha,$$

donc ψ est bien un \mathbb{F}_q -automorphisme. Par ailleurs, pour $\alpha \in \mathbb{F}_{q^m}$, on a

$$\psi^m(\alpha) = \varphi^{nm}(\alpha) = \alpha^{p^{nm}} = \alpha,$$

donc $\psi^m = \text{Id}$. Soit d l'ordre de ψ . Par ce qui précède, d divise m (et donc $d \leq m$). Pour tout $\alpha \in \mathbb{F}_{q^m}$ on a

$$\alpha = \psi^d(\alpha) = \varphi^{dn}(\alpha) = \alpha^{p^{dn}},$$

donc tout élément de \mathbb{F}_{q^m} est racine du polynôme $g = X^{p^{dn}} - X$, donc $p^{dn} \geq |\mathbb{F}_{q^m}| = p^{nm}$. Ceci implique que $d \geq m$, donc $d = m$. On a donc que ψ est un élément de $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ d'ordre m . Reste à montrer qu'il engendre $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

On raisonne par récurrence sur m . Supposons que $m = 1$. On a alors $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \text{Gal}(\mathbb{F}_q/\mathbb{F}_q) = \{\text{Id}\}$ et $\psi = \text{Id}$, donc ψ engendre $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

On suppose que $m \geq 2$ plus l'hypothèse de récurrence. On choisit $\alpha_0 \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$. Soit $h \in \mathbb{F}_q[X]$ le polynôme minimal de α_0 et d son degré. On a $d \geq 2$ car $\alpha_0 \notin \mathbb{F}_q$. De plus $[\mathbb{F}_q(\alpha_0) : \mathbb{F}_q] = d$ et $\{1, \alpha_0, \dots, \alpha_0^{d-1}\}$ est une base de $\mathbb{F}_q(\alpha_0)$ sur \mathbb{F}_q . Par ailleurs, soient $\alpha_0, \alpha_1, \dots, \alpha_{r-1}$ les racines de h qui sont incluses dans $\mathbb{F}_q(\alpha_0)$. Pour tout $\rho \in \text{Gal}(\mathbb{F}_q(\alpha_0)/\mathbb{F}_q)$, il existe $i \in \{0, 1, \dots, r-1\}$ tel que $\rho(\alpha_0) = \alpha_i$. Par ailleurs, pour $i \in \{0, 1, \dots, r-1\}$, il existe au plus un $\rho \in \text{Gal}(\mathbb{F}_q(\alpha_0)/\mathbb{F}_q)$ tel que $\rho(\alpha_0) = \alpha_i$. En effet, si $\rho, \rho' \in \text{Gal}(\mathbb{F}_q(\alpha_0)/\mathbb{F}_q)$ sont tels que $\rho(\alpha_0) = \rho'(\alpha_0) = \alpha_i$, alors $(\rho^{-1} \circ \rho')(\alpha_0) = \alpha_0$, donc $(\rho^{-1} \circ \rho')(\alpha_0^k) = \alpha_0^k$ pour tout $k \in \{0, 1, \dots, d-1\}$, donc $\rho^{-1} \circ \rho' = \text{Id}$ car $\{1, \alpha_0, \dots, \alpha_0^{d-1}\}$ est une base de $\mathbb{F}_q(\alpha_0)$ vu comme espace vectoriel sur \mathbb{F}_q et $\rho^{-1} \circ \rho'$ est linéaire sur \mathbb{F}_q . D'où $\rho = \rho'$. Ceci montre que

$$|\text{Gal}(\mathbb{F}_q(\alpha_0)/\mathbb{F}_q)| \leq r \leq d.$$

Par ailleurs, comme $|\mathbb{F}_q(\alpha_0)| = q^d$, on a $\mathbb{F}_q(\alpha_0) \simeq \mathbb{F}_{q^d}$, donc, par ce qui précède, $\{\psi^k; 0 \leq k \leq d-1\}$ est un sous-ensemble de $\text{Gal}(\mathbb{F}_q(\alpha_0)/\mathbb{F}_q)$ de cardinal d . Il en résulte que

$$\text{Gal}(\mathbb{F}_q(\alpha_0)/\mathbb{F}_q) = \{\psi^k; 0 \leq k \leq d-1\}.$$

Considérons l'extension $\mathbb{F}_q(\alpha_0) = \mathbb{F}_{q^d} \subset \mathbb{F}_{q^m}$. Posons $d' = [F_{q^m} : \mathbb{F}_{q^d}]$. On a

$$q^m = |\mathbb{F}_{q^m}| = |\mathbb{F}_{q^d}|^{d'} = q^{dd'},$$

donc $m = dd'$. De plus, comme $d \geq 2$, on a $d' < m$. Par hypothèse de récurrence, il s'en suit que $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_{q^d})$ est un groupe cyclique d'ordre d' engendré par $\varphi^{nd} = \psi^d$.

Soit $\rho \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Pour tout $\alpha \in \mathbb{F}_q(\alpha_0) = \mathbb{F}_{q^d}$ on a

$$\rho(\alpha)^{q^d} - \rho(\alpha) = \rho(\alpha^{q^d} - \alpha) = \rho(0) = 0,$$

donc $\rho(\alpha) \in \mathbb{F}_{q^d}$. D'où $\rho(\mathbb{F}_{q^d}) \subset \mathbb{F}_{q^d}$. Par ce qui précède, on sait qu'il existe $k \in \{0, 1, \dots, d-1\}$ tel que $\rho|_{\mathbb{F}_{q^d}} = \psi^k|_{\mathbb{F}_{q^d}}$. Posons $\rho' = \rho \circ \psi^{-k}$. On a $\rho'|_{\mathbb{F}_{q^d}} = \text{Id}$, donc $\rho' \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_{q^d})$. Par ce qui précède, il existe $l \in \{0, 1, \dots, d'-1\}$ tel que $\rho' = (\psi^d)^l = \psi^{ld}$. Finalement, $\rho = \rho'\psi^k = \psi^{k+ld}$. Ceci montre que $\text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ est engendré par ψ . \square

Corollaire 10.3. Soient p un nombre premier et n un entier ≥ 1 . Posons $q = p^n$. Alors $\text{Gal}(\mathbb{F}_q)$ est un groupe cyclique d'ordre n engendré par l'automorphisme de Frobenius.

Démonstration. Soit $\rho \in \text{Gal}(\mathbb{F}_q)$. On a $\rho(1) = 1$, donc

$$\rho(k) = \rho(1 + 1 + \dots + 1) = \rho(1) + \rho(1) + \dots + \rho(1) = 1 + 1 + \dots + 1 = k$$

pour tout $k \in \mathbb{F}_p$, donc $\rho|_{\mathbb{F}_p} = \text{Id}$, c'est-à-dire $\rho \in \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Ceci montre que $\text{Gal}(\mathbb{F}_q) = \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Par le théorème 10.2 il s'en suit que $\text{Gal}(\mathbb{F}_q)$ est un groupe cyclique d'ordre n engendré par $\varphi^1 = \varphi$, où φ désigne l'automorphisme de Frobenius. \square