I. Anneaux de fractions

Dans ce chapitre A désigne un anneau intègre (unitaire, différent de $\{0\}$, et sans diviseur de zéro).

1. Construction des anneaux de fractions

Définition 1. On dit qu'une partie S de A est multiplicative si $1 \in S$, $0 \notin S$ et si $x\,y \in S$ pour tout x, y de S.

Exemples.
– $S = A \setminus \{0\}$, car A est intègre.
– $S = A^*$.
– $S = A \setminus \mathfrak{p}$ où $\mathfrak{p}$ est un idéal premier de A (en particulier $\neq A$). Comme $\mathfrak{p}$ est différent de A on a $1 \notin \mathfrak{p}$ et donc $1 \in S$. De même $0 \in \mathfrak{p}$ et donc $0 \notin S$. Si $x, y \in S$ alors $x \notin \mathfrak{p}$ et $y \notin \mathfrak{p}$ puis $xy \notin S$ et donc $xy \in S$.

Sur le produit $S \times A$ on considère la relation $(s, a) \sim (s', a')$ si $s\,a' = s'\,a$.

Lemme 2. La relation $\sim$ est une relation d'équivalence sur $S \times A$.

Démonstration. La réfléxivité et la symmétrie de $\sim$ sont immédiates. Soient $(s, a), (s', a'), (s'', a'')$ des éléments de $S \times A$ tels que $(s, a) \sim (s', a')$ et $(s', a') \sim (s'', a'')$. De la commutativité de A et des relations $sa' = s'a$ et $s''a' = s'a''$, on obtient

$$s's''a = s''s'a = s''sa' = s''a's = s'a''s = s'sa'',$$

puis $s'(s''a - sa'') = 0$. Comme s' est dans S, qui ne contient pas 0, et que A est un anneau intégre, on a $s''a = sa''$ puis $(s, a) \sim (s'', a'')$. La relation $\sim$ est donc transitive. □

On note $S^{-1}A$ l'ensemble des classes d'équivalences de $S \times A$ modulo $\sim$, c'est-à-dire $S^{-1}A = (S \times A)/\sim$.

Proposition 3. Les opérations

$$\begin{array}{rcl} o_+ : (S \times A)^2 & \to & (S \times A) \\ (s_1, a_1), (s_2, a_2) & \mapsto & (s_1 s_2, s_1 a_2 + s_2 a_1) \end{array} \qquad \begin{array}{rcl} o_\times : (S \times A)^2 & \to & (S \times A) \\ (s_1, a_1), (s_2, a_2) & \mapsto & (s_1 s_2, a_1 a_2) \end{array}$$

sont compatibles avec la relation $\sim$.

Démonstration. Le rôle de (s_1, a_1) et (s_2, a_2) étant symétrique, les opérations o_+ et $o_\times$ sont commutatives. Il est donc suffisant d'établir $o_+((s_1', a_1'), (s_2, a_2)) \sim o_+((s_1, a_1), (s_2, a_2))$ et $o_\times((s_1', a_1'), (s_2, a_2)) \sim o_\times((s_1, a_1), (s_2, a_2))$ pour $(s_1', a_1') \sim (s_1, a_1)$. De $(s_1', a_1') \sim (s_1, a_1)$ on obtient $s_1' a_1 = s_1 a_1'$. On a

$$\begin{aligned} o_\times((s_1', a_1'), (s_2, a_2)) \sim o_\times((s_1, a_1), (s_2, a_2)) &\Leftrightarrow (s_1' s_2, a_1' a_2) \sim (s_1 s_2, a_1 a_2) \\ &\Leftrightarrow s_1' s_2 a_1 a_2 = s_1 s_2 a_1' a_2. \end{aligned}$$

Encore par $s_1' a_1 = s_1 a_1'$ on obtient $s_1' s_2 a_1 a_2 = s_1' a_1 s_2 a_2 = s_1 a_1' s_2 a_2 = s_1 s_2 a_1' a_2$. Le cas de o_+ est traité à l'exercice 1 du TD 2. □

On peut ainsi définir les deux lois internes suivantes sur $S^{-1}A$:

$$\begin{array}{rcl} +_{S^{-1}A} : \overline{S^{-1}A \times S^{-1}A} & \to & \overline{S^{-1}A} \\ \overline{(s_1, a_1)}, \overline{(s_2, a_2)} & \mapsto & \overline{(s_1 s_2, s_1 a_2 + s_2 a_1)} \end{array} \qquad \begin{array}{rcl} \times_{S^{-1}A} : \overline{S^{-1}A \times S^{-1}A} & \to & \overline{S^{-1}A} \\ \overline{(s_1, a_1)}, \overline{(s_2, a_2)} & \mapsto & \overline{(s_1 s_2, a_1 a_2)} \end{array}$$

Théorème 4. Muni des lois $+_{S^{-1}A}$, $\times_{S^{-1}A}$, l'ensemble $S^{-1}A$ est un anneau commutitatif unitaire. L'application $i = i_{S^{-1}A} : a \mapsto \overline{(1,a)}$ est un morphisme d'anneau injectif de A dans $S^{-1}A$. De plus pour tout $s \in S$, l'élément $\overline{(s,1)}$ est inversible d'inverse $\overline{(1,s)}$.

Démonstration. A l'aide de fastidieux calculs on montre directement que $(S^{-1}A, +_{S^{-1}A}, \times_{S^{-1}A})$ est un anneau commutatif ayant $0_{S^{-1}A} = \overline{(1,0)}$ comme neutre et $1_{S^{-1}A} = \overline{(1,1)}$ comme unité et que i est un morphisme injectif d'anneau. Soit $s \in S$ alors $\overline{(s,1)}$ et $\overline{(1,s)}$ sont des éléments de $S^{-1}A$ vérifiant la relation $\overline{(s,1)}\overline{(1,s)} = \overline{(1,1)} = 1_{S^{-1}A}$. Quelques uns des axiomes seront établis à l'exercice 2 du TD 2. □

Corollaire 5. Pour $S = A \setminus \{0\}$ l'anneau $S^{-1}A$ est un corps, appelé *corps des fractions* de A.

Démonstration. Soit a et s des éléments de $S = A \setminus \{0\}$. On on a $\overline{(s,a)}\overline{(a,s)} = \overline{(sa,as)} = 1_{S^{-1}A}$. Les autres couples (a,b) de $S \times A$ sont obtenus avec $a = 0$ et $s \in S$. De $\overline{(s,0)} = 0_{S^{-1}A}$ on obtient alors $\left(S^{-1}A\right)^* = S^{-1}A \setminus \{0_{S^{-1}A}\}$ et donc $S^{-1}A$ est un corps. □

Les éléments $\overline{(s,a)}$ du corps des fractions de A sont notés $\frac{a}{s}$ avec $a \in A$ et $s \in A \setminus \{0\}$.

Proposition 6. Soit S une partie multiplicative de A, B un anneau et $f : A \to B$ un morphisme d'anneaux tel que $f(S) \subseteq B^*$. Il existe un unique morphisme $\varphi : S^{-1}A \to B$ tel qu'on ait la relation $f = \varphi \circ i_{S^{-1}A}$. De plus $\varphi\left(\overline{(s,a)}\right) = f(s)^{-1}f(a)$.

Démonstration. Supposons que φ existe. Alors pour $\frac{a}{s} \in S^{-1}A$, on a

$$\begin{aligned}\varphi\left(\overline{(s,a)}\right) &= \varphi\left(\overline{(s,1)}\,\overline{(1,a)}\right) = \varphi\left(\overline{(s,1)}\right)\varphi\left(\overline{(1,a)}\right) = \varphi\left(\overline{(1,s)}^{-1}\right)\varphi\left(\overline{(1,a)}\right)\\ &= \varphi\left(\overline{(1,s)}\right)^{-1}\varphi\left(\overline{(1,a)}\right) = \varphi(i(s))^{-1}\varphi(i(a)) = f(s)^{-1}f(a).\end{aligned}$$

Ainsi, si le morphisme φ existe, il est unique. Montrons que l'application $\varphi : S^{-1}A \to B$ définie par $\varphi\left(\frac{a}{s}\right) = f(s)^{-1}f(a)$ est bien définie et que c'est un morphisme d'anneaux. Comme $f(S) \subseteq B^*$, le symbole $f(s)^{-1}f(a)$ existe pour tout $(s,a) \in S \times A$. Montrons que $f(s)^{-1}f(a)$ ne dépendant pas du représentant de $\overline{(s,a)}$. Soit (s,a) et (s',a') deux couples de $S \times A$ vérifiant la relation $(s,a) \sim (s',a')$. On a

$$\begin{aligned}f(s')^{-1}f(a') &= f(s')^{-1}f(s)^{-1}f(s)f(a') = f(s')^{-1}f(s)^{-1}f(sa') = f(s')^{-1}f(s)^{-1}f(s'a)\\ &= f(s')^{-1}f(s)^{-1}f(s')f(a) = f(s')^{-1}f(s')f(s)^{-1}f(a) = f(s)^{-1}f(a).\end{aligned}$$

La fonction φ est donc bien définie. On montre immédiatement que φ est un morphisme d'anneau (unitaire). □

Proposition 7. Soit K le corps de fraction de A et S une parie multiplicative de A, l'anneau $S^{-1}A$ est isomorphe à un sous-anneau de K formé des éléments $\frac{a}{s}$ avec $a \in A$ et $s \in S$.

Démonstration. Posons $i = i_K : A \to K$ et $j = i_{S^{-1}A} : A \to S^{-1}A$. Les éléments de $K \setminus \{0_K\}$ étant inversible dans K il en est de même de $i(S)$, car $0 \notin S$. Par la Proposition 6, il existe un morphisme d'anneaux $\varphi : S^{-1}A \to K$ définie par $\varphi(\overline{(s,a)}) = i(s)^{-1}i(a)$ et vérifiant $i = \varphi \circ j$. Soit $\overline{(s,a)}$ un élément de $\ker(\varphi)$. Alors $0 = \varphi(\overline{(s,a)}) = i(s)^{-1}i(a)$. Comme $i(s)^{-1}$ est non nul et K intègre, on a $i(a) = 0$ puis $a = 0$ par injectivité de i. De $\overline{(s,0)} = \overline{(1,0)} = 0_{S^{-1}A}$ on obtient que φ est injective. Ainsi $S^{-1}A$ est isomorphe a $\varphi(S^{-1}A)$ qui est un sous anneaux de K. De plus $\varphi(\overline{(s,a)}) = i(s)^{-1}i(a) = \frac{1}{s}\frac{a}{1} = \frac{a}{s}$ pour tout $(s,a) \in S \times A$. □

On peut ainsi identifier tous les anneaux de fractions de A comme sous-anneaux du corps de fraction de A.

Exemple. Pour $A = \mathbb{Z}$ et $S = \{10^k \mid k \in \mathbb{Z}\}$, l'anneau de fraction $S^{-1}A$ est l'anneau des nombres décimaux de $\mathbb{Q}$.

2. Un critère d'irréductibilité

Proposition 8. Soit A un anneau factoriel, K son corps de fraction. Si $F \in A[X]$ n'est pas le produit de deux polynômes de $A[X]$ de degré ≥ 1 alors F est irréductible dans $K[X]$.

Proposition 9. Supposons F réductible dans $K[X]$. Il existe alors F et G dans $K[X]$ tels que $F = GH$ avec $\deg(G) \geq 1$ et $\deg(H) \geq 1$. Soit a un multiple commun des dénominateurs des coefficients de G. On a alors $a \in A$ et $G_1 = aG \in A[X]$. De même il existe $b \in A$ tel que $H_1 = bH \in A[X]$. On a ainsi obtenu la reduction $abF = G_1H_1$ dans $A[X]$. Comme A est factoriel, il existe $u \in A^*$ et $p_1, \ldots, p_n$ des éléments irréductibles de A tels que $ab = up_1 \cdots p_n$. On rappel que les irréductibles de A sont irréductibles dans $A[X]$ (lemme de Gaußß). De p_1 divise abF on obtient p_1 divise G_1 ou H_1. Si p_1 divise G_1 on note G_2 le polynôme de $A[X]$ vérifiant $G_1 = p_1G_2$ et on pose $H_2 = H_1$. Si p_1 ne divise pas G_1 alors il divise H_1, on pose alors $G_2 = G_1$ et $H_1 = pH_2$. On obtient alors $up_2 \cdots p_nF = G_2H_2$ dans $A[X]$. En continuant ainsi pou $p_2, \ldots, p_n$ on arrive à $uF = G_nH_n$ dans $A[X]$. Finalement on pose $G' = u^{-1}G_n \in A[X]$ et $H' = H$, ce qui donne $F = G'H'$ dans $A[X]$ et donc F est réductible dans $A[X]$. On a ainsi établit la contraposée de la proposition.

Théorème 10 (Critère d'Einsenstein)**.** Soit A un anneau factoriel de corps de fraction K,

$$F = a_nX^n + \cdots + a_1X + a_0$$

un polynôme de $A[X]$ de degré $n \geq 1$ et p un irréductible de A. On suppose $p \nmid a_n$, $p \mid a_i$ pour $0 \leq i < n$ et $p^2 \nmid a_0$ alors F est irréductible dans $A[X]$ et donc dans $K[X]$.

Démonstration. Supposons qu'il existe deux polynômes non constants G et H de $A[X]$ tels que $F = GH$. On pose

$$G = b_qX^q + \cdots + b_1X + b_0, \quad \text{et} \quad H = c_rX^r + \cdots + c_1X + c_0,$$

avec $q = \deg G \geq 1$ et $r = \deg H \geq 1$. On a $a_0 = b_0c_0$. Ainsi p divise exactement un seul des entiers b_0 et c_0. Quitte a échanger G et H on peut supposer $p \mid c_0$ et $p \nmid b_0$. Puisque $a_n = b_qc_r$ n'est pas divisible par p, le coefficient c_r n'est pas divisible par p. Soit k le plus petit entier tel que $p \nmid c_k$. On a nécessairement $k \leq r < n$. En posant $b_i = 0$ pour $i > q$, on obtient

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + c_kb_0.$$

Comme p ne divise pas b_0c_k mais tous les autres termes de la somme, on $p \nmid a_k$ ce qui est impossible. □

3. Résultant

Définition 11. Soit A un anneau commutatif, $F = a_nX^n + \cdots + a_1X + a_0$ et $G = b_mX^m + \cdots + b_1X + b_0$ des polynômes de $A[X]$ de degré n et m strictement positif. La matrice de Sylvester de F et G est

$$\mathrm{Syl}(F,G) = \begin{bmatrix} a_n & 0 & \ldots & \ldots & 0 & b_m & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \vdots & \vdots & & \ddots & 0 \\ a_0 & & & \ddots & 0 & \vdots & & & b_m \\ 0 & \ddots & & & a_n & b_0 & & & \vdots \\ \vdots & \ddots & \ddots & & \vdots & 0 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & \ldots & 0 & a_0 & 0 & \ldots & 0 & b_0 \end{bmatrix} \in M_{n+m}(\mathbb{K}).$$

Le déterminant de la matrice $\mathrm{Syl}(F,G)$ est noté $\mathrm{Res}(F,G)$, c'est le *résultant* des polynômes F et G.

Théorème 12. Soit A un anneau factoriel et F, G deux polynômes de $A[X]$. Alors $\mathrm{Res}(F,G)=0$ si et seulement si $F \wedge G \neq 1$.

Démonstration. Exercice 3 du TD 2. □

Définition 13. On appelle discriminant d'un polynôme F de degré $n \geq 2$

$$\Delta(F) = \frac{(-1)^{\frac{n(n-1)}{2}}}{a_n} \mathrm{Res}(F, F'),$$

où a_n est le coefficient de plus haut degré de F.

Remarque 14. Certains auteurs posent directement $\Delta(F) = \mathrm{Res}(F, F')$.

Corollaire 15. Soit k un corps de caractéristique 0. Un polynôme F de $k[X]$ de degré ≥ 2 admet une racine multiple dans une clôture algébrique de k si et seulement si $\Delta(F) = 0$.

Démonstration. Exercice 3 du TD 2. □

Dans le corollaire précédent le corps est de caractéristique non nul pour pouvoir utiliser le critère : F admet une racine multiple (dans une clôture algébrique) de k si et seulement si $\mathrm{pgcd}(F, F') \neq 1$.

II. Extension de corps

Rappel : Soit A un anneau commutatif et I un idéal de A.
– I est premier si A/I est un anneau intègre (en particulier unitaire) ;
– I est maximal si A/I est un corps ;
– si A est principal, l'idéal I est premier $\neq \{0\}$ si et seulement s'il est maximal.

Soit A un anneau intègre. Il existe un unique morphisme d'anneaux $c : \mathbb{Z} \to A$ tel que $c(1) = 1_A$. On a alors

$$c(n) = \underbrace{1_A + \cdots + 1_A}_{n \text{ fois}} \quad \text{et} \quad c(-n) = \underbrace{(-1_A) + \cdots + (-1_A)}_{n \text{ fois}}.$$

L'image de c est un sous-anneau de A qui est intègre et est donc lui aussi intègre. Par ailleurs on a $\mathbb{Z}/\ker(c) \sim \mathrm{Im}(c)$ et donc $\mathbb{Z}/\ker(c)$ est intègre. Il en suit que $\ker(c)$ est un idéal premier de $\mathbb{Z}$. On a donc $\ker(c) = 0$ où $\ker(c) = p\mathbb{Z}$ avec p un nombre premier. L'anneau A contient donc un sous anneau isomorphe à exactement l'un des anneau $\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z}$.

Définition 1. Soit A un anneau intègre. On dit que A est de *caractéristique* 0 s'il contient un sous-anneau isomorphe à $\mathbb{Z}$ et de *caractéristique* p s'il contient un sous-anneau isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Dans le cas où A est en particulier un corps, on a que A contient une copie de $\mathbb{Q}$ (cas de la caractéristique nulle) ou une copie de $\mathbb{F}_p$ (cas de la caractéristique p). On parle de *sous-corps premier*.

1. Extension de corps

Définition 2. Etant donnée deux corps L et K, on dit que L/K est une extension si K est inclus dans L. On dit aussi que L est une extension de K.

On prendra garde à ne pas confondre l'extension L/K avec un quotient.

Exemples. $\mathbb{C}/\mathbb{R}$ est une extension de corps. Si $\mathbb{Q}(T)$ est le corps des fractions rationnelles à une indéterminée, $\mathbb{Q}(T)/\mathbb{Q}$ est une extension de corps.

Proposition 3. Si L/K est une extension de corps, alors L est muni naturellement d'une extension de K-espace vectoriel.

Démonstration. La loi $+$ est celle du corps L. On définit la multiplication scalaire par

$$\begin{array}{rcl} \cdot : K \times L & \to & L \\ (\lambda, y) & \mapsto & \lambda \cdot_L y, \end{array}$$

qui est bien défini car $K \subset L$. On vérifie alors immédiatement qu'on munit ainsi L d'une structure de K-espace vectoriel. □

Définition 4. Soit L/K une extension de corps. Si L n'est pas finiment engendré comme K-espace vectoriel, on pose $[L : K] = +\infty$ sinon $[L : K] = \dim_K(L)$. C'est le *degré* de L/K. Si $[L : K] < +\infty$, on dit que L/K est une *extension finie*.

Exemple. On a $[\mathbb{C} : \mathbb{R}] = 2$ et $[\mathbb{Q}(T) : \mathbb{Q}] = +\infty$.

Théorème 5. Soit $K \subseteq L \subseteq M$ des corps, $(e_i)_{1 \leq i \leq n}$ une base de L sur K et $(f_j)_{1 \leq j \leq m}$ une base de M sur L. Alors la famille $(e_i f_j)_{i,j}$ est une base de M sur K.

Démonstration. Montrons que la famille $(e_i f_j)_{i,j}$ est K-libre. Soient $a_{i,j}$ avec $1 \leq i \leq n$ et $1 \leq j \leq m$ des éléments de K vérifiant $\sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j} e_i f_j = 0$. On a

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j} e_i f_j = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{i,j} e_i f_j = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{i,j} e_i \right) f_j = \sum_{j=1}^{m} \alpha_j f_j.$$

La famille $(f_j)_{1 \leq j \leq m}$ étant libre sur L tandis que les α_j sont des éléments de L. Ainsi pour $j \in \{1, .., n\}$ on obtient

$$\alpha_j = \sum_{i=1}^{n} a_{i,j} e_i = 0$$

Comme la famille (e_i) est une base, on obtient $a_{1,j} = \cdots = a_{n,j} = 0$. Finalement on a montré $a_{i,j} = 0$ pour tout $1 \leq i \leq n$ et $1 \leq j \leq m$.

Montrons que la famille $(e_i f_j)_{i,j}$ est K-génératrice de L. Soit x un élément de M. Comme (f_j) est une famille L-génératrice de M il existe $(b_j)_j$ dans L vérifiant $x = \sum_{j=1}^{m} b_j f_j$. Soit $j \in \{1, \ldots, m\}$. Le coefficient b_j est un élément de L. Comme (e_i) est une famille génératrice il existe $(a_{i,j})_i$ de K tels qu'on ait $b_j = \sum_{i=1}^{n} a_{i,j} e_i$ et donc

$$x = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{i,j} e_i f_j.$$

La famille $(e_i\, f_j)_{i,j}$ étant libre et génératrice, c'est une K-base de M. □

Corollaire 6. Soit M/L et L/K deux extensions de corps. Si $[M : L]$ et $[L : K]$ sont finies alors $[M : K]$ est finie et on a la relation $[M : K] = [M : L][L : K]$.

Définition 7. Soit L/K une extension de corps et S une partie de L. On note $K(S)$ le plus petit sous-corps de L contenant K et S.

Lemme 8. Soit L/K une extension, S une partie de L. Le sous-corps $K(S)$ est la réunion des $K(\Sigma)$ où Σ parcours les parties finies de S :

$$K(S) = \bigcup_{\substack{\Sigma \subseteq S \\ \mathrm{card}(\Sigma) < +\infty}} K(\Sigma)$$

Démonstration. Notons K' la réunion des $K(\Sigma)$. Comme $A \subseteq B$ implique $K(A) \subseteq K(B)$, on obtient que K' est incluse dans $K(S)$. Montrons l'inclusion réciproque. Pour cela il suffit de montrer que K' est un sous-corps de L contenant K et S. Comme K' contient K, on a $\{0, 1\} \subseteq K'$. Soient x_1 et x_2 deux éléments de K'. Il existe alors $\Sigma_1, \Sigma_2 \subseteq S$ tel que $x_1 \in K(\Sigma_1)$ et $x_2 \in K(\Sigma_2)$ avec Σ_1 et Σ_2 finis. Posons $\Sigma = \Sigma_1 \cup \Sigma_2$. On a donc $x_1, x_2 \in K(\Sigma)$ et ainsi $x + y$, $-x$ et xy sont dans $K(\Sigma) \subseteq K'$. L'ensemble K' est donc un corps contenant K. De

$$S \subseteq \sum_{s \in S} K(\{s\}) \subseteq K',$$

on obtient $K(S) \subseteq K'$. □

Définition 9. Si S est finie, $S = \{\alpha_1, \ldots, \alpha_r\}$, on note $K(\alpha_1, \ldots, \alpha_r)$; l'extension L/K est dite *monogène* s'il existe $\alpha \in L$ tel que $L = K(\alpha)$.

2. Eléments algébriques

Soit L/K une extension de corps et α un élément de L. On définit l'homomorphisme d'évaluation

$$\begin{array}{rcl} \mathrm{ev}_\alpha : K[X] & \to & L \\ F & \mapsto & F(\alpha) \end{array}$$

Comme L est intègre, l'image de ev_α est donc aussi intègre. De $\mathrm{Im}(\mathrm{ev}_\alpha) \sim K[X]/\ker(\mathrm{ev}_\alpha)$, on obtient que $\ker(\mathrm{ev}_\alpha)$ est un idéal premier de $K[X]$. On a donc soit $\ker(\mathrm{ev}_\alpha) = (0)$ ou bien il existe un polynôme P irréductible et unitaire dans $K[X]$ tel que $\ker(\mathrm{ev}_\alpha) = (P)$.

Définition 10. Soit L/K une extension de corps, α un élément de L. Si $\ker(\mathrm{ev}_\alpha) = (0)$ on dit que α est *transcendant* sinon α est dit *algébrique*, le polynôme unitaire P engendrant $\ker(\mathrm{ev}_\alpha)$ est alors le polynôme *minimal* de α sur K, on le note $\mathrm{Irr}(\alpha, K)$.

Exemple. Dans l'extension $\mathbb{C}/\mathbb{R}$, tout élément $x = a + ib$ avec $a, b \in \mathbb{R}$ est algébrique sur $\mathbb{R}$: si $b = 0$, il est racine de $X - a$, si $b \neq 0$ il est racine de $X^2 - (2a)X + a^2 + b^2$ et c'est deux polynôme sont irréductibles sur $\mathbb{R}$.

Proposition 11. Soit M/L et L/K des extensions de corps et $\alpha \in M$ un élément algébrique sur K. Alors α est aussi algébrique sur L.

Démonstration. Il existe un polynôme irréductible de $K[X]$ tel que $P(\alpha) = 0$. De $K \subseteq L$, on peut considérer $P \in L[X]$. Il existe alors un diviseur irréductible Q de P dans $L[X]$ tel que $Q(\alpha) = 0$. Il en suit que α est algébrique sur L. □

Corollaire 12. Soit L/K une extension de corps et x, y deux éléments de L avec y algébrique sur K. Alors y est algébrique sur $K(x)$.

Théorème 13. Soit K/L une extension de corps et $\alpha \in L$. Les propriétés suivantes sont équivalentes :
- $i)$ α est algébrique sur K,
- $ii)$ $K(\alpha) = K[\alpha]$,
- $iii)$ $[K(\alpha) : K] < +\infty$, plus précisément $[K(\alpha) : K] = \deg(\mathrm{Irr}(\alpha, K)$.

Démonstration. Montrons $i) \Rightarrow ii)$ On a $K[\alpha] = \mathrm{Im}(\mathrm{ev}_\alpha)$ puis $\mathrm{Im}(\mathrm{ev}_\alpha) \sim K[X]/(P)$. Comme P est irréductible, l'idéal (P) est premier puis maximal (car $K[X]$ principal) et donc $K[X]/(P)$ est un corps. Il en suit que $K[\alpha]$ est un corps contenu dans $K(\alpha)$ et contenant K et α. On a donc $K[\alpha] = K(\alpha)$.

Montrons $ii) \Rightarrow i)$. Par ce qui précède on a soit $K[\alpha] = K[X]/(P)$ avec P irréductible soit $K[\alpha]$ est isomorphe à $K[X]$. Or $K[X]$ n'est pas un corps tandis que $K(\alpha)$ en est un. On a donc forcément $K[\alpha] = K[X]/(P)$ et α est algébrique sur K.

Montrons $ii) \Rightarrow iii)$. Par $ii) \Rightarrow i)$ on a que α est algébrique sur K. Posons $n = \deg(\mathrm{Irr}(\alpha, K))$. En tant que K-espace vectoriel, $K[\alpha]$ a pour base la famille $(1, \alpha, \ldots, \alpha^{n-1})$. Ainsi de $K(\alpha) = K[\alpha]$ on obtient $[K(\alpha) : K] = n = \deg(\mathrm{Irr}(\alpha, K))$.

Montrons $iii) \Rightarrow ii)$. Posons $n = [K(\alpha) : K]$. La famille $1, \alpha, \ldots, \alpha^n$ est donc liée. Il existe ainsi un polynôme P de degré au plus n tel que $P(\alpha) = 0$. L'élément α est donc algébrique sur K. De $i) \Rightarrow ii) \Rightarrow iii)$ on obtient $n = [K(\alpha) : K] = \deg(\mathrm{Irr}(\alpha, K))$. □

Corollaire 14. Soient L/K une extension $\alpha \in L$ un élément algébrique. La famille $(1, \alpha, \ldots, \alpha^{n-1})$ est une K-base de $K(\alpha)$ avec $n = [K(\alpha) : K] = \deg_K(\mathrm{Irr}(\alpha, K))$.

Démonstration. Montrons que c'est une famille libre. Soit $\lambda_0, \ldots, \lambda_{n-1}$ des éléments de K tels qu'on ait $\sum_{i=0}^{n-1} \lambda_i \alpha^i = 0$. Posons $Q(X) = \sum_{i=0}^{n-1} \lambda_i X^i$. On a alors $\deg(Q) \leq n - 1$ et $Q(\alpha) = 0$. De $n = \deg(\mathrm{Irr}(\alpha, K))$ on obtient $Q = 0$ et donc $\lambda_0 = \cdots = \lambda_{n-1} = 0$. La famille $1, \alpha, \ldots, \alpha^{n-1}$ est donc libre. Comme elle est de cardinalité n, c'est une base de $K(\alpha)$ sur K. □

Quand on parle d'élément algébrique (resp. transcendant) sans plus de précision il s'agit de nombres complexes algébrique (resp. transcendant) sur $\mathbb{Q}$.

Définition 15. On dit qu'une extension de corps L/K est *algébrique* si tout élément de L est algébrique sur K.

Proposition 16. Si l'extension de corps L/K est finie alors elle est algébrique.

Démonstration. Soit $\alpha \in L$. Le sous anneau $K[\alpha]$ est un sous K-espace vectoriel de L. Comme le degré $[L : K] = \dim_K(L)$ est fini, on a que $\dim_K K[\alpha]$ est aussi fini. On conclut par le théorème 13. □

Attention la réciproque est fausse en générale.

Théorème 17. Soient L/K et M/L deux extensions de corps telles que L/K soit algébrique et x un élément de M algébrique sur L. Alors x est algébrique sur K.

Démonstration. Soit $P \in L[X]$ le polynôme minimal de x sur L. Ecrivons $P = \sum_{i=0}^{n} a_i X^i$. On a donc $a_i \in L$ pour $i = 0, \ldots, n-1$ et $a_n = 1$. Considérons la suite de corps

$$K = K_0 \subseteq K_1 = K(a_0) \subseteq \cdots \subseteq K_i = K(a_0, \ldots, a_{i-1}) \subseteq \cdots \subseteq K_n = K(a_0, \ldots, a_{n-1}).$$

Pour chaque i le coefficient a_i est algébrique sur K (car L/K est algébrique) et donc aussi sur K_i. L'extension K_{i+1}/K_i est donc algébrique et monogène. Le degré $[K_{i+1} : K_i]$ est donc fini (c'est le degré du polynôme minimal de a_i sur K_i). Comme les coefficients a_i sont dans K_n, l'élément x est algébrique sur K_n et donc l'extension $[K_t(x) : K_n]$ est algébrique et de degré finie. Par le corollaire 6 on obtient

$$[K_n(x) : K] = [K_t(x) : K_n] \times [K_n : K_{n-1}] \times \cdots \times [K_2 : K_1] \times [K_1 : K] < +\infty$$

Par la proposition 16, l'extension $K_n(x)/K$ est algébrique et donc x est algébrique sur K. □

Corollaire 18. Soient M/L et L/K deux extensions algébriques. Alors M/K est une extension algébrique.

Démonstration. Tout élément x de M est algébrique dur L et donc sur K par le théorème précédent. □

Corollaire 19. Soit L/K une extension, x et y deux éléments de L algébriques sur K. Alors $x + y$ et xy sont algébriques sur K.

Démonstration. Considérons le sous corps $K(x, y)$ de L. On a $K(x, y) = K(x)(y)$ et l'extension $K(y)/K$ est algébrique. L'élément x est algébrique sur K et donc en particulier sur $K(y)$ par la proposition 11. On obtient donc que $K(x)(y) = K(x, y)$ est algébrique sur K. On conclut en remarquant que $x + y$ et $x \times y$ sont dans $K(x, y)$. □

Corollaire 20. Soit K un corps et P un polynôme irréductible dans $K[X]$. Posons $L = K[X]/(P)$ et identifions K et son image dans L (c'est-à-dire $K \subseteq L$). Alors L/K est une extension algébrique.

Démonstration. Le corps L est un K-espace vectoriel de dimension finie. L'extension L/K est donc algébrique par la proposition 16. □

Corollaire 21. Soient M/K une extension et L l'ensemble des x de M algébrique sur K. Alors L est une extension algébrique de K.

Démonstration. Par le corollaire 19, l'ensemble L est un sous-anneau de M. Soit $x \in L \setminus \{0\}$. On a $K(x) \subseteq L$ avec $K(x)$ corps, d'ou $x^{-1} \in K(x) \subseteq L$. L'anneau L est donc un corps contenant K. Comme tout élément de L est algébrique sur K, c'est une extension algébrique de K. □

III. Extensions normales et séparables

Nous allons nous intéresser à deux problèmes. Etant donné un polynôme $P \in K[X]$:

– construire une extension L de K dans laquelle P possède une racine a,

– construire une extension M de K dans laquelle P se décompose en un produit de polynômes de degré 1.

1. Corps de rupture - Corps de décomposition

Pour le premier problème, on peut se restreindre aux polynômes irréductibles de degré > 1.

Définition 1. Soit K un corps et $P \in K[X]$ un polynôme irréductible. Une extension L/K est un *corps de rupture* de P sur K si L est monogène, $L = K(\alpha)$, avec $P(\alpha) = 0$.

Théorème 2. Soit $P \in K[X]$ irréductible. Il existe un corps de rupture pour P sur K, unique à isomorphisme près.

Démonstration. Montrons l'existence. On prend $L = K[X]/(P)$, c'est un corps puisque P est irréductible. On pose $\alpha = \overline{X}$ et $n = \deg(P)$. Comme K-espace vectoriel, L admet la base $(1, \alpha, \ldots, \alpha^{n-1})$. Par construction on a $P(\alpha) = P(\overline{X}) = \overline{P(X)} = 0$ et donc $L = K(\alpha)$. Pour l'unicité, on va démontrer le résultat suivant. □

Lemme 3. Soient K, K' deux corps, i un isomorphisme du corps K sur K' et P un polynôme irréductible de $K[X]$. On pose $P' = i(P)$ (ses coefficients sont images de ceux de P par i). Soit $L = K(\alpha)$ un corps de rupture de P sur K et $L' = K'(\alpha')$ un corps de rupture de P' sur K'. Il existe un unique isomorphisme φ de L sur L' tel que $\varphi(\alpha) = \alpha'$ et $\varphi|_K = i$.

Démonstration. On prolonge i en un isomorphisme de $K[X]$ sur $K'[X]$ en posant $i(X) = X$. L'image de l'idéal (P) est $(i(P))$. On en déduit un morphisme $\bar{i}$ entre les quotients $K[X]/(P)$ et $K'[X]/(i(P))$. Comme $K[X]/(P)$ est un corps, l'isomorphisme $\bar{i}$ est injectif. Les K-espaces vectoriels $K[X]/(P)$ et $K'[X]/(i(P))$ étant de même dimension finie, $\bar{i}$ est un isomorphisme. En posant $u(\overline{X}) = \alpha$ on construit un morphisme de $K[X]/(P)$ dans $L = K(\alpha)$ vérifiant $u|_K = \mathrm{id}_K$. Ce morphisme est injectif (comme tout morphisme de corps) et surjectif, c'est donc un isomorphisme. De même on a isomorphisme u' de $K'[X]/(i(P))$ dans $L' = K'(\alpha')$ vérifiant $u'(\overline{\overline{X}}) = \alpha'$. On pose alors $\varphi = u' \circ \bar{i} \circ u^{-1}$. On vérifie la relation $\varphi|_K = \bar{i}|_K = i$ ainsi que

$$\varphi(\alpha) = u'(\bar{i}(u^{-1}(\alpha))) = u'(\bar{i}(\overline{X})) = u'(\overline{\overline{X}}) = \alpha'.$$

De $L = K(\alpha)$, on obtient que φ est entièrement déterminée par les conditions $\varphi(\alpha) = \alpha'$ et $\varphi|_K = i$. D'où l'unicité. □

Fin démonstration du théorème. On pose $K = K'$ et $i = \mathrm{id}_K$ et donc $P' = P$. □

Remarque 4. Si L est corps de rupture sur K de P, ce dernier peut ne pas être entièrement factorisé sur L : par exemple $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ est un corps de rupture sur $\mathbb{Q}$ de $X^3 - 2$ mais ne contient pas ses deux autres racines non réelles $\sqrt[3]{2}j$ et $\sqrt[3]{2}j^2$. Si M/K est une extension, M peut contenir plusieurs corps de rupture du même polynôme P : les sous-corps $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}j)$ et $\mathbb{Q}(\sqrt[3]{2}j^2)$ de $\mathbb{C}$ sont trois corps de rupture distincts pour $X^3 - 2$ sur $\mathbb{Q}$.

Définition 5. Soient L, L' deux extensions d'un corps K, on appelle K-isomorphisme de L sur L' tout isomorphisme de corps de L sur L' dont la restriction sur K est l'identité. Dans le cas où $L = L'$ on parle de K-automorphisme.

Définition 6. Soit $P \in K[X]$ (irréductible ou non) de degré $n \geq 1$. Un *corps de décomposition* de P sur K est une extension L de K telle que :
– dans $L[X]$, P est un produit de polynôme de degré 1,
– L est minimal pour cette propriété (i.e. L est engendré par les racines de P).

Théorème 7. Pour tout polynôme $P \in K[X]$ de degré ≥ 1, il existe un corps de décomposition, unique à isomorphisme près.

Démonstration. Montrons l'existence. On procède par récurrence sur le degré n de P. Si $n = 1$, le corps K convient. Supposons l'existence d'un corps de décomposition établie pout tout corps M et tout polynômes de $M[X]$ de degré $\leq n$. Soit $P \in K[X]$ de degré $n+1$ et Q un facteur irréductible de P. Soit K' un corps de rupture de Q et x une racine de Q dans K'. On a donc $K' = K(x)$. Dans K' on a $P = (X-x)R(X)$. Comme $\deg(R) = n < \deg(P)$, le polynôme R admet un corps de décomposition L sur K'. Notons $y_1, \ldots, y_n$ les racines de R. Ainsi $L = K'(y_1, \ldots, y_n) = K(x, y_1, \ldots, y_n)$ est corps de décomposition de P. Pour l'unicité on va démontrer un résultat plus précis. □

Lemme 8. Soient K et K' deux corps, i un isomorphisme de K dans K', P un polynôme de $K[X]$. Soient L un corps de décomposition de P sur K, L' un corps de décomposition sur K' de $P' = i(P) \in K'[X]$. Il existe un isomorphisme φ de L dans L' qui prolonge i.

Démonstration. On raisonne par récurrence sur le degré de P. Si $\deg(P) = 1$ alors $L = K$ et $L' = K'$ et on pose alors $\varphi = i$. Supposons le résultat établi pour tout corps M, tout polynôme de $M[X]$ de degré $\leq n$ et tout isomorphisme η. Soit P un polynôme de degré $n+1$. Soit $\alpha \in L$ une racine de P. Elle est racine d'un facteur irréductible Q de P. Posons $Q' = i(Q)$; c'est un facteur irréductible de P'. Comme L' est corps de décomposition de P' il existe $\alpha' \in L'$ racine de Q'. Les corps $K(\alpha)$ et $K'(\alpha')$ sont corps de ruptures de Q et Q' sur K et K' respectivement. Soit ψ l'isomorphisme de $K(\alpha)$ sur $K'(\alpha')$ qui prolonge i et vérifiant $\psi(\alpha) = \alpha'$. On a

$$R' = P'/(X - \alpha') = i(P)/(\psi(X) - \psi(\alpha)) = \psi(P)/\psi(X - \alpha) = \psi(P/(X - \alpha)) = \psi(R).$$

Les polynômes R et R' sont de degré n. Les corps L et L' sont corps de décomposition de R et $R' = \psi(R)$ sur $K(\alpha)$ et $K'(\alpha') = \psi(K(\alpha))$ respectivement. Par hypothèse de récurrence il existe donc un isomorphisme φ de L dans L' qui prolonge ψ et donc i. □

Fin démonstration du théorème. On pose $K = K'$ et $i = \mathrm{id}_K$. On a alors $P = P'$. □

Définition 9. Soit K un corps, une extension $\overline{K}$ est une clôture algébrique de K si :
– $\overline{K}$ est algébriquement clos,
– $\overline{K}$ est algébrique sur K.

On a montré en exercice l'existence d'une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ dans $\mathbb{C}$. Attention $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$.

Théorème 10 (Steinitz 1910)**.** Tout corps K admet une clôture algébrique. Si Ω et Ω' sont deux clôtures algébriques de K, il existe un K-isomorphisme de Ω sur Ω'.

Démonstration. Admise. □

Corollaire 11. Soit K un corps, Ω une clôture algébrique de K et E/K une extension algébrique finie. Il existe un K-isomorphisme de E sur un sous corps de Ω.

2. Extensions normales

Soit K un corps et Ω une clôture algébrique de K fixée une fois pour toute.

Définition 12. On dit que deux éléments x et x' de Ω sont *conjugués* sur K s'ils ont le même polynôme minimal sur K.

Si $K(x)$ et $K(x')$ sont des corps de rupture d'un même polynôme P, il existe d'après le lemme 3, un K-isomorphisme de $K(x)$ sur $K(x')$ tel que $\varphi(x) = x'$. Réciproquement étant donné deux éléments x et x' de Ω. S'il existe un K-isomorphisme ψ de $K(x)$ dans un corps L tel que $\psi(x) = x'$ alors les corps $K(x)$ et $K(x')$ sont K-isomorphes. Il en suit que les éléments x et x' ont le même polynôme minimal : si $P = \mathrm{Irr}(x, K)$ alors on a

$$0 = \psi(0) = \psi(P(x)) = P(\psi(x)) = P(x'),$$

et donc $\mathrm{Irr}(x', K)$ divise P. Comme on a aussi que $\mathrm{Irr}(x, K)$ divise $\mathrm{Irr}(x', K)$, on obtient $\mathrm{Irr}(x, K) = \mathrm{Irr}(x', K)$.

Définition 13. Une extension algébrique L/K est dite normale si elle contient tous les conjugués se chacun de ses éléments.

Ainsi si L/K et une extension normale et $x \in L$, toutes les racines de $\mathrm{Irr}(x, K)$ sont dans L.

Exemples.

– Une extension quadratique L/K est normale.

– Une extension cubique n'est pas toujours normale : si $K = \mathbb{Q}$ et $L = \mathbb{Q}(x)$ où x est une racine de $X^3 - 2$, l'extension L/K n'est pas normale. Par contre si $K = \mathbb{Q}(j)$ et $L = K(x)$ et $L = K(x)$ où x racine de $X^3 - 2$ alors L/K est une extension normale.

Proposition 14. Si L/K est une extension finie, pour qu'elle soit normale, il faut et il suffit que L soit le corps de décomposition d'un polynôme de $K[X]$.

Démonstration. Supposons que L/K soit normale et de degré fini n. Soient $x_1, \ldots, x_n$ une K-base de L et $F = \prod_{i=1}^{n} \mathrm{Irr}(x_i, K)$. Le polynôme $\mathrm{Irr}(x_i, K)$ ayant x_i comme racine dans L, toutes ses racines sont dans L (car L est normale). Ainsi $\mathrm{Irr}(x_i, K)$ est produits d'irréductible de degré 1 dans $L[X]$. Il existe donc $y_1, \ldots, y_m \in L$ tels que $F = \prod_{i=1}^{m}(X - y_i)$. On a alors

$$L = K(x_1, \ldots, x_k) \subseteq K(y_1, \ldots, y_m) \subseteq K(x_1, \ldots, x_m) = L.$$

Il en suit que L est le corps de décomposition de F.

Réciproquement. Supposons $L = K(x_1, \ldots, x_n)$ où les x_i sont les racines d'un polynôme P. Posons $d = [L : K]$. Pour tout i, l'élément x_i est algébrique de degré $\leq d$. Nous avons donc $x_i^d \in K(1, \ldots, x_i^{d-1})$. Soit Q un polynôme irréductible de $K[X]$ ayant une racine x dans L. Soit x' une autre racine de Q dans Ω. Par le lemme 3, il existe un K-isomorphisme ψ de $K(x)$ sur $K(x')$ vérifiant $\psi(x) = x'$. Comme x est un élément de L, il existe $\lambda_{1,1}, \ldots, \lambda_{1,d}, \ldots, \lambda_{n,1}, \ldots, \lambda_{n,d}$ tels qu'on ait

$$x = \sum_{i=1}^{n} \sum_{j=0}^{d-1} \lambda_{i,j} x_i^j.$$

On a alors $x' = \psi(x) = \sum_{i=1}^{n} \sum_{j=0}^{d-1} \lambda_{i,j} \psi(x_i)^j$. Posons $P = \sum_{i=0}^{n} a_i X^i$. On a alors

$$P(\psi(x_i)) = \sum_{i=0}^{n} a_i \psi(x_i)^i = \sum_{i=0}^{n} a_i \psi(x_i^i) = \psi(P(x_i)) = 0,$$

et donc $\psi(x_i)$ est une racine de P. L'isomorphisme ψ envoie donc les racines de P sur les racines de P il en suit que $x' = \psi(x)$ est une combinaison K-linéaire des x_i^j puis $x' \in L$. □

Corollaire 15. Toute extension finie L de K peut se plonger dans une extension normale finie M de K.

Démonstration. Soient L/K une extension finie et $x_1, ..., x_n$ une K-base de L. Comme pour la démonstration de la proposition on construit $F = \prod_{i=1}^{n} \mathrm{Irr}(x_i, K)$. Le corps de décomposition de F contient L et est donc normale. □

3. Séparabilité

Définition 16. Un élément algébrique sur un corps K est dit *séparable* sur K si son polynôme minimal admet des racines toutes distinctes dans un corps de décomposition. Un élément qui n'est pas séparable est dit *inséparable*. Une extension algébrique est dite *séparable* si tous ses éléments sont séparables, *inséparable* sinon.

Exemple. Soit $K = \mathbb{F}_2(X)$. Le polynôme $P = Y^2 - X$ de $K[Y]$ est irréductible car de degré 2 et sans racine dans K. Soit α une racine de K. Dans $K(\alpha)[Y]$ on a $Y^2 - X = Y^2 - \alpha^2 = (Y - \alpha)^2$ et donc α n'est pas séparable sur $\mathbb{K}$.

Soit α un élément non séparable sur K, $P = \mathrm{Irr}(\alpha, K)$ et L un corps de décomposition de P. Le polynôme P admet une racine multiple, il existe donc β dans L tel que $P(\beta) = P'(\beta) = 0$. Par minimalité de P, P' est un multiple de P. De $\deg(P') < \deg(P)$ on obtient alors $P = 0$.

Corollaire 17. Les éléments algébrqiques sur un corps K de caractéristique 0 sont toujours séparables. Toute extension d'un corps de caractéristique 0 est séparable.

Définition 18. On dit qu'un corps K est *parfait* si toute extension algébrique de K est séparable.

Tout corps de caractéristique 0 est parfait. Le corps $\mathbb{F}_2(X)$ n'est pas parfait.

Lemme 19. Soient L/K une extension finie, x un élément de Ω, φ un automorphimse de L et M une extension normale finie contenant L. Le nombre n de L-isomorphismes de $L(x)$ dans un sous-corps de M prolongeant φ est le nombre de L-conjugués de x dans M. En particulier n est inférieur ou égale à $[L(x) : L]$. De plus on a $n = [L(x) : L]$ si et seulement si x est séparable.

Démonstration. Posons $L' = L(x)$ et notons $y_1, \ldots, y_k$ les L-conjugués distincts de x dans M. Le corps L' étant corps de rupture de $P = \mathrm{Irr}(x, L)$, le lemme 3 garantit l'existence d'un unique isomorphisme ψ de $L(x)$ dans $L(y_i) \subset M$ prolongeant φ et vérifiant $\psi(x) = y_i$. On a donc $n = k \leq d = [K(x) : K]$. On conlut en remarquant qu'on a $k = d$ si et seulement si x est séparable. □

Théorème 20. Le nombre n de K-isomorphismes distincts d'une extension L/K finie à valeur dans une extension normale finie M contenant L est inférieur ou égal à $[L : K]$. De plus $n = [L : K]$ si et seulement si L est engendré par des éléments séparables.

Démonstration. Posons $L = K(x_1, \ldots, x_r)$. Pour $i = 1, \ldots, r$ on pose $L_i = K(x_1, \ldots, x_i)$. On a ainsi $L_i = L_{i-1}(x_i)$. Posons $d_i = [L_i : L_{i-1}]$. Soit φ un automorphisme de L_{i-1}. En notant n_i le nombre d'automorphismes de L_i dans M prolongeant φ, le lemme 19 garantit $n_i \leq d_i$ avec égalité si et seulement si x_i est séparable. On conclut en observant $[L : K] = \prod_{i=1}^{r} d_i$ et que le nombre de K-isomorphismes de L est $\prod_{i=1}^{r} n_i$. □

Corollaire 21. Une extension L/K engendrée par une famille d'éléments séparables sur K est séparable sur K.

Démonstration. Soit M une extension normale finie de K contenant L. Soit x_1 un élément de L. Il existe alors $x_2, \ldots, x_n$ vérifiant $L = K(x_1, \ldots, x_n)$. Comme L/K est engendrée par des éléments séparables il y'a exactement $[L : K]$ K-isomorphsimes de L à valeur dans M. La démonstration précédente implique que ceci est possible si et seulement si les x_i sont tous séparable, en particulier x. □

Corollaire 22. Une extension L/K séparable finie peut être plongée dans une extension normale séparable finie.

Démonstration. Posons $L = K(x_1, \dots, x_n)$. Les éléments x_i sont séparables. On note M le corps de décomposition dans Ω de

$$F = \prod_{i=1}^{n} \mathrm{Irr}(x_i, K).$$

L'extension M est alors engendrée par les racines de F qui sont tous séparables. L'extension normale M/K est donc séparable. □

Corollaire 23. Soit L/K une extension normale séparable finie. Les K-automorphisme de L forment un groupe et sont au nombre de $[L : K]$.

Démonstration. On utilise le Théorème 20 avec $M = L$. □

4. Élément primitif

Lemme 24. Si un K-espace vectoriel E est la réunion d'une famille finie de sous K-espaces vectoriels distincts de E alors K est fini.

Démonstration. Supposons que E soit la réunion des sous K-espaces vectoriels $F_1, \dots, F_n$ distintcs et différents de E. Quitte à en retirer, on peut aussi supposer $F_i \not\subseteq F_j$ pour $i \neq j$. Soit u un vecteur de F_1 n'appartenant pas aux autres F_i et v un vecteur de $E \setminus F_1$. Alors l'ensemble $v + Ku$ est disjoint de F_1 et contient au plus un vecteur des autres F_i. Si $x = v + \lambda u$ et $y = v + \mu u$ sont dans F_i avec $\mu \neq \lambda$ alors $\frac{1}{\lambda - \mu}(x - y) = u \in F_i$. Par conséquent K a au plus $n - 1$ éléments. □

Théorème 25 (de l'élément primitf)**.** Soit L une extension finie d'un corps K de caractéristique nulle. Il existe un élément $\alpha \in L$ tel que $L = K(\alpha)$.

Démonstration. Le corps K étant de caractéristique nulle, l'extension L/K est séparable. Posons $n = [L : K]$. Pour $n = 1$, il n'y a rien à montrer. Supposons donc $n \geq 2$. Soit $M \subseteq \Omega$ une extension normale finie contenant L. Par le théorème 20 il y'a alors n K-isomorphismes u_i distincts de K dans M. Posons $V_{i,j} = \{x \in L \,|\, u_i(x) = u_j(x)\}$, sous K-espace vectoriel de L distinct de L. Comme K est infini, le lemme 24 garantit que L est différent de la réunion des $V_{i,j}$. Il existe donc $\alpha \in L \setminus (\cup_{1 \leq i < j \leq n} V_{i,j})$. Posons $P = \mathrm{Irr}(\alpha, K)$ et $P = \sum_{k=0}^{m} a_k X^k$ avec $m \leq n$. Soit $i \in \{1, \dots, n\}$. On a

$$P(u_i(\alpha)) = \sum_{k=0}^{m} a_k u_i(\alpha)^k = \sum_{k=0}^{m} u_i\left(a_k \alpha^k\right) = u_i\left(\sum_{k=0}^{m} a_k \alpha^k\right) = u_i(P(\alpha)) = u_i(0) = 0.$$

et donc $u_i(\alpha)$ est racines de P. Par construction de α, P a donc au moins n racines. La sous-extension $K(\alpha)$ de L est donc de degré n sur K. Par conséquent $L = K(\alpha)$. □

Une version en caractéristique p du théorème de l'élément primitf sera démontrée en TD.

IV. Théorie de Galois

1. Théorème d'Artin

Dans cette section L/K et M/L sont des extensions et H est un ensemble isomorphismes distincts de L dans M

Définition 1. L'ensemble $L^H = \{x \in L\,,\, \varphi(x) = x \text{ pour tout } \varphi \in H\}$ est un sous-corps de L appelé *sous-corps de L fixé par H*.

Le fait que L^H soit un sous-corps de L est une conséquence directe du fait que les éléments de H soient des isomorphismes de L.

Lemme 2 (Dedekind)**.** Si H est fini alors ses éléments sont M-linéairement indépendants.

Démonstration. Par récurrences sur le cardinal n de H. Evident pour $n = 1$. Supposons le résultat établi pour $n - 1 \geq 1$ et montrons le pout n. Posons $H = \{\varphi_1, \ldots, \varphi_n\}$. Supposons par l'absurde qu'il existe $a_1, \ldots, a_n \in M$ non tous nuls tels que $\sum_{i=1}^n a_i\varphi_i = 0$. Quitte à renumérotter les φ_i on peut supposer $a_1 \neq 0$.

Soit $y \in L$ tel que $\varphi_1(y) \neq \varphi_n(y)$ et $x \in L$ quelconques. On a alors

$$\begin{aligned}
0 &= a_1\varphi_1(xy) + \cdots + a_n\varphi_n(xy) - \varphi_n(y)(a_1\varphi_1(x) + \cdots + a_n\varphi_n(x)) \\
0 &= a_1\varphi_1(x)\varphi_1(y) + \cdots + a_n\varphi_n(x)\varphi_n(y) - a_1\varphi_1(x)\varphi_n(y) - \cdots - a_n\varphi_n(x)\varphi_n(y) \\
0 &= a_1(\varphi_1(y) - \varphi_n(y))\varphi_1(x) + \cdots + a_{n-1}(\varphi_{n-1}(y) - \varphi_n(y))\varphi_{n-1}(x).
\end{aligned}$$

En posant $b_i = a_i(\varphi_i(y) - \varphi_n(y))$ on obtient $\sum_{i=1}^n b_i\varphi_i = 0$ avec $b_1 \neq 0$, ce qui contredit l'hypothèse de récurrence. □

Théorème 3 (Artin)**.** Soient L/K et M/L deux extensions et $H = \{\varphi_1, \ldots, \varphi_n\}$ une famille de n isomorphismes de L à valeur dans M distincts. On a $[L : L^H] \geq n$ et l'égalité est atteinte si H est un groupe.

Démonstration. Supposons par l'absurde qu'on ait $[L : L^H] = p < n$. En tant que L^H-espace vectoriel L admet donc une base $\{x_1, \ldots, x_p\}$. Le système de p équations et $n > p$ inconnues $a_1, \ldots, a_n$.

$$\sum_{j=1}^{n} a_j\varphi_j(x_i) = 0, \quad \text{pour } j = 1, \ldots, p. \tag{4.1}$$

possède une solution non triviale. Il existe donc $a_1, \ldots, a_n$ de M non tous nuls tels que $a_1\varphi_1 + \cdots + a_n\varphi_n = 0$. Ceci est impossible par le Lemme de Dedekind. On a donc $[L : L^H] \geq n$.

Supposons maintenant que H soit un groupe. Les éléments de H sont donc à valeurs dans L et on peut supposer $M = L$. Soient $x_1, \ldots, x_{n+1}$ des éléments de L. Le système de n équations

$$a_1\varphi_i(x_1) + \cdots + a_{n+1}\varphi_i(x_{n+1}) = 0, \quad 1 \leq i \leq n, \tag{4.2}$$

et $n + 1$ inconnues a_i à une solution non triviale. Notons r le nombre minimal de a_i non nuls parmi les solutions non triviale du système. Quitte à renumérotter les φ_i et à diviser la solution par a_1, on peut supposer qu'il existe une solution $(a_1, \ldots, a_{n+1})$ vérifiant

$$a_1 = 1, a_2 \neq 0, \ldots, a_r \neq 0, a_{r+1} = 0, \ldots, a_{n+1} = 0,$$

avec r minimal parmi toutes les solutions possibles. Soit φ un élément de H. Comme H est un groupe il existe $\sigma \in \mathfrak{S}_n$ tel qu'on ait $\varphi \circ \varphi_i = \varphi_{\sigma(i)}$ pour tout $i = 1, \ldots, n$. Les équations (4.2) deviennent alors

$$\varphi(a_1)\varphi_{\sigma(j)}(x_1) + \cdots + \varphi(a_r)\varphi_{\sigma(j)}(x_r), \quad 1 \leq j \leq n, \tag{4.3}$$

En retranchant (4.2) et (4.3) pour $j = \sigma^{-1}(i)$, on obtient

$$(a_1 - \varphi(a_1))\varphi_i(x_1) + (a_2 - \varphi(a_2))\varphi_i(x_2) + \cdots + (a_r - \varphi(a_r))\varphi_i(x_r) = 0.$$

Comme a_1 vaut 1, on a $\varphi(a_1) = \varphi(1) = 1 = a_1$ et donc

$$(a_2 - \varphi(a_2))\varphi_i(x_2) + \cdots + (a_r - \varphi(a_r))\varphi_i(x_r) = 0 \quad \text{pour } i = 1, ..., n,$$

On a ainsi obtenu une solution de (4.2) avec au plus $r - 1$ termes non nulles. On a donc forcément $\varphi(a_i) = a_i$ pour $i = 2, \ldots, r$ puis $\varphi(a_i) = a_i$ pour $i = 1, \ldots, n + 1$. Il en suit $\{a_1, \ldots, a_{n+1}\} \in L^H$. Comme H est un groupe l'un des φ_i est l'identité sur L, notons le φ_k. On a alors

$$a_1 x_1 + \cdots + a_{n+1} x_{n+1} = 0$$

avec $a_i \in L^H$ et $(a_1, \ldots, a_{n+1}) \neq 0$. La famille $(x_1, \ldots, x_{n+1})$ n'est donc pas libre, ce qui implique l'inégalité $[L^H : K] \leq n$. □

2. Extensions galoisiennes

Définition 4. Une extension finie L/K est dite *galoisienne* si elle est normale et séparable. Le groupe des K-automorphismes de L s'appelle le *groupe de Galois* de L/K noté $\mathrm{Gal}(L/K)$. Si L/K est une extension séparable, la plus petite extension galoisienne (qui existe par le corollaire III.22) qui la contient est la *clôture galoisienne* de L sur K.

Si L/K est galoisienne et $\mathrm{Gal}(L/K)$ est cyclique (resp. abélien) on dit que l'extension est cyclique (resp. abélienne) ; ce transfert de vocabulaire se généralise à d'autres types de groupes.

Proposition 5. Soit M/K une extension galoisienne et L un sous-corps de M contenant K alors M/L est une extension galoisienne.

Démonstration. L'extension M/L est clairement finie et séparable. Montrons qu'elle est normale. Soit x un élément de M. Notons $P = \mathrm{Irr}(x, K)$ et $Q = \mathrm{Irr}(x, L)$. De $K \subseteq L$ on a $P \in L[X]$ et donc P est un multiple de Q. L'extension M/K étant normale elle contient toutes les racines de P et en particulier celles de Q. L'extension M/L est donc normale. □

Théorème 6. Pour que l'extension finie L/K soit galoisienne, il faut et il suffit que K coïncide avec le corps des éléments invariants par le groupe de tous les K-automorphismes de L.

Démonstration. Notons H l'ensemble des K-automorphismes de L. Supposons que L/K soit galoisienne de degré n. Comme L/K est séparable et normale le Corollaire III.23 implique que H est un groupe et qu'on a $\mathrm{card}(H) = n$. Le Théorème d'Artin impliquant $[L : L^H] = n$ avec $K \subset L^H$, on obtient $L^H = K$.

Réciproquement, soit L/K une extension finie de degré n, G le groupe des K-automorphismes de L, on suppose que $K = L^G$. On pose $G = \{\sigma_1, \ldots, \sigma_n\}$ avec $\sigma_1 = \mathrm{id}$. Par le théorème de l'élément primitif il existe $x \in L$ tel que $L = K(x)$. Le théorème d'Artin garantit alors $\mathrm{card}(G) = [L : K] = n$. Pour $i = 1, \ldots, n$ on pose $x_i = \sigma_i(x)$. Pour $i \neq j$ on a $x_i \neq x_j$ car sinon $\sigma_i(x) = \sigma_j(x)$ avec $\sigma_i|_K = \sigma_j|_K = \mathrm{id}_K$ et donc $\sigma_i = \sigma_j$. On construit alors le polynôme

$$P = \prod_{i=1}^{n} (X - x_i) = \sum_{i=1}^{n} a_i X^i.$$

Soit $\sigma \in G$, en posant $\sigma(X) = X$, on obtient

$$\sigma(P) = \prod_{i=1}^{n}(X - \sigma(x_i)) = \prod_{i=1}^{n}(X - (\sigma \circ \sigma_i)(x)) = P \quad \text{et} \quad \sigma(P) = \sum_{i=1}^{n} \sigma(a_i)X^i.$$

On a donc $\sigma(a_i) = a_i$ pour tout $\sigma \in G$. Par définition de G, on a donc $a_i \in K$. Le polynôme P est donc dans $K[X]$. On rappel $P(x) = P(x_1) = 0$. L'extension L est engendré par x et contient toutes les racines de P. Le corps L est donc corps de décomposition de P. L'extension L/K est donc normale. Les éléments x_i étant tous distincts, P n'a pas de racines multiples et donc les x_i sont séparables. L'extension $L = K(x)$ est donc engendré par un élément séparable, elles est donc séparable par le Corollaire III.21. □

Corollaire 7. Soit M/K une extension galoisienne, l'application qui à une sous-extension L de M/K associe $\mathrm{Gal}(M/L)$ est injective.

Démonstration. Soit L tel $K \subseteq L \subseteq M$. Par la proposition 5, l'extension M/L est galoisienne et L est le corps des invariants de $\mathrm{Gal}(M/L)$. Notons η l'application définie par $\eta(L) = \mathrm{Gal}(M/L)$ et μ l'application de $\mathcal{P}(\mathrm{Gal}(L/H))$ définie par $\mu(H) = M^H$. On a alors $(\mu \circ \eta)(L) = L$. L'application $\mu \circ \eta$ est donc l'identité et η est injective. □

Si L est un corps et H, G sont deux ensembles d'isomorphismes de L dans Ω vérifiant $H \subseteq G$ alors on a $L^G \subseteq L^H$. De plus les éléments de H sont des L^H-isomorphismes.

Théorème 8 (Premier théorème de Galois)**.** Soit M/K est une extension galoisienne finie. Il existe une bijection entre les sous-extension de M/K et les sous-groupes de $\mathrm{Gal}(L/K)$. Cette bijection est donné par $L \mapsto \mathrm{Gal}(M/L)$ et a pour réciproque $H \mapsto M^H$.

Démonstration. Notons η l'application définie par $\eta(L) = \mathrm{Gal}(M/L)$. Grâce au Corollaire 7, nous savons que η est injective. Montrons que η est surjective. Soit H un sous-groupe de $G = \mathrm{Gal}(M/K)$. On a alors $H \subseteq \mathrm{Gal}(M/M^H)$. Le théorème d'Artin implique $[M : M^H] = \mathrm{card}(H)$ tandis que le théorème III.20 établit que $\mathrm{Gal}(M/M^H)$ est de cardinal $[M : M^H]$. On obtient ainsi $H = \mathrm{Gal}(M/M^H)$ et donc $\eta(M^H) = H$. On vient ainsi de montrer que l'application η est bijective. Si on compose η avec l'application μ définie par $\mu(M^H) = H$ on obtient l'identité comme dans la preuve du corollaire 7. L'application μ est don bien la réciproque de η. □

Lemme 9. Soit M/K une extension galoisienne. Pour tout corps intermédiaire L entre K et M, et tout élément g de $\mathrm{Gal}(M/K)$, on a :

$$\mathrm{Gal}(M/g(L)) = g\,\mathrm{Gal}(M/L)g^{-1}.$$

Démonstration. Soit $h \in \mathrm{Gal}(M/L)$ et $x \in L$, on a

$$(g \circ h \circ g^{-1})(g(x)) = (g \circ h)(x) = g(h(x)) = g(x).$$

Ainsi ghg^{-1} laisse fixe les éléments de $g(L)$, d'où $g\,\mathrm{Gal}(M/L)g^{-1} \subseteq \mathrm{Gal}(M/g(L))$. Par ailleurs on a

$$\begin{aligned}\mathrm{card}(g\,\mathrm{Gal}(M/L)g) = \mathrm{card}(\mathrm{Gal}(M/L)) = [M : L] &= \frac{[M : K]}{[L : K]} \\ &= \frac{[M : K]}{[g(L) : K]} = [M : g(L)] = \mathrm{card}(\mathrm{Gal}(M/g(L)),\end{aligned}$$

et donc $\mathrm{Gal}(M/g(L)) = g\,\mathrm{Gal}(M/L)g^{-1}$. □

Soit L/K une extension finie, M la clôture normale de K contenant L, x un élément de L. Notons $x = x_1, \ldots, x_n$ les conjugués de x. Par le lemme III.19, les K-isomorphismes de L dans M sont les morphismes $\varphi_1, \ldots, \varphi_n$ définies par $\varphi_i|_K = \mathrm{id}_K$ et $\varphi_i(x) = x_i$.

Théorème 10 (Second théorème de Galois)**.** Soit M/K une extension galoisienne et L un corps intermédiaire entre K et M. L'extension L/K est galoisienne si et seulement si $\mathrm{Gal}(M/L)$ est distingué dans $\mathrm{Gal}(M/K)$ et alors

$$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(M/K)/\mathrm{Gal}(M/L).$$

Démonstration. L'extension L/K est séparable car M/K l'est. Pour que L/K soit normale il faut et il suffit que L contienne tous les conjugués de ses éléments et donc que tous les conjugués de L soit dans L. Soit x un élément de L. L'ensemble des conjugués de x est alors $\{g(x) \mid g \in \mathrm{Gal}(M/K)\}$. Ainsi L/K est galoisienne si et seulement si $g(L) = L$ pour tout $g \in \mathrm{Gal}(L/K)$. D'où L/K est galoisienne si et seulement si $\mathrm{Gal}(M/L) = \mathrm{Gal}(M/g(L)) = g\,\mathrm{Gal}(M/L)g^{-1}$ pour tout $g \in \mathrm{Gal}(M/K)$ et donc si et seulement si $\mathrm{Gal}(M/L)$ est distingué dans $\mathrm{Gal}(M/K)$. □

3. Extensions cyclotomiques

Soit K un corps de clôture algébrique Ω et $n \in \mathbb{N} \setminus \{0\}$. On considère le polynôme $P_n = X^n - 1$. La dérivée de P_n est nX^{n-1}. Ainsi si la caractéristique p de K ne divise pas n, le polynôme P n'a pas de racines multiples. Dans la suite on supposer a toujours que c'est le cas.

On note $U_n(K)$ les racines de P_n dans K : $U_n(K) = \{x \in K \mid x^n = 1\}$. C'est un sous groupe de K^* pour la multiplication, de cardinal $\leq n$, il est donc cyclique. Pour la suite K_n désigne le corps de décomposition de P_n.

Proposition 11. $U_n(\mathbb{K})$ est un un sous groupe cyclique de K^* isomorphe à $\mathbb{Z}/d\mathbb{Z}$ avec $d|n$.

Démonstration. On montre immédiatement que $U_n(K)$ est un sous-groupe. Il est fini car P_n a au plus n racines dans K. Comme tout sous-groupe fini du groupe multiplicatif d'un corps, $U_n(K)$ est cyclique. On a $U_n(K) \subseteq U_n(\Omega)$ et ce dernier est de cardinal n. On obtient alors que $U_n(K_n)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ puis que $U_n(K)$ est un sous groupe cyclique de $\mathbb{Z}/n\mathbb{Z}$ il est donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Par le théorème de Lagrange on a alors $d|n$. □

Définition 12. On appelle *racine primitive n-ième* de l'unité tout générateur de $U_n(K_n)$ et on note $U_n^*(K_n)$ leur ensembles.

Le groupe $\mathbb{Z}/n\mathbb{Z}$ admettant $\varphi(n)$ on obtient $\mathrm{card}(U_n^*(K_n)) = \varphi(n)$.

Définition 13. Le n-ème *polynôme cylcotomique* $\Phi_{n,K} \in K_n[X]$ est donné par :

$$\Phi_n = \prod_{\zeta \in U_n^*(K_n)} (X - \zeta)$$

Le polynôme Φ_n est unitaire de degré $\varphi(n)$.

Proposition 14. On a l'identité

$$X^n - 1 = \prod_{d|n} \Phi_d$$

Démonstration. Tout élément de $U_n(K)$ est d'ordre un diviseur de n. On a donc $U_n(K) = \bigsqcup_{d|n} U_d^*(K)$ puis l'égalité polynomiale désirée. □

Lemme 15. Soit A un anneau et $P \in A[X]$, $P \neq 0$, de coefficient dominant inversible. Pout tout $F \in A[X]$ il existe $Q, R \in A[X]$ tels qu'on ait $F = PQ + R$ et $\deg(R) < \deg(P)$.

Démonstration. On peut supposer que P est un polynôme unitaire. On pose $P = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$. On considère l'anneau quotient $B = A[X]/(P)$. Soit $\overline{X}$ l'image de X dans B. Il suffit alors de montrer que tout élément de B est combinaison linéaire en $1, \overline{X}, ..., \overline{X}^{n-1}$. Il suffit de le faire pour les monômes. On conclut en remarquant $\overline{X}^n = -a_{n-1}\overline{X}^{n-1} - ... - a_1\overline{X} - a_0$ □

Proposition 16. On a les propriétés suivantes :
– i) Le polynôme $\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$.
– ii) Soit k un corps quelconque et $\sigma : \mathbb{Z} \to k$ l'homorphisme tel que $\sigma(1) = 1$. On a alors

$$\Phi_{n,k} = \sigma\left(\Phi_{n,\mathbb{Q}}\right)$$

En particulier $\Phi_{n,\mathbb{F}_p}$ s'obtient de $\Phi_{n,\mathbb{Q}}$ par réduction modulo p.

Démonstration. i) On raisonne par récurrence sur n. On a $\Phi_{1,\mathbb{Q}} = X-1 \in \mathbb{Z}[X]$. Supposons la propriété vraie pour tout $d < n$. Posons $P = \prod_{d|n,d<n} \Phi_{d,\mathbb{Q}}$ est un polynôme unitaire à coefficients dans $\mathbb{Z}$. Par le lemme précédent il existe F et R de $\mathbb{Z}[X]$ tel qu'on ait $\deg(R) < \deg(P)$ et $X^n - 1 = FP + R$. Mais on a $X^n - 1 = \Phi_{n,\mathbb{Q}}P$ dans $\mathbb{Q}[X]$, donc $P(\Phi_{n,\mathbb{Q}} - P) = R$ et pour une raison de degré on a nécessairement, on a $\Phi_{n,\mathbb{Q}} = F \in \mathbb{Z}[X]$.

ii) On raisonne par récurrence, le cas $n = 1$ étant trivial. Dans $\mathbb{Z}[X]$, on a

$$X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{Q}} = \Phi_{n,\mathbb{Q}}P.$$

Comme σ est un homomorphisme, on a dans $K_n[X]$: $X^n - 1 = \sigma(X^n - 1) = \sigma(\Phi_{n,\mathbb{Q}})\sigma(P)$. Mais, par hypothèse de récurrence, on a

$$\sigma(P) = \prod_{d|n,d<n} \sigma(\Phi_{d,\mathbb{Q}}) = \prod_{d|n,d<n} \Phi_{d,k}$$

et comme on a, par définition, $X^n - 1 = \prod_{d|n} \Phi_{d,k}$ il en résulte, puisque $k[X]$ est intègre, qu'on a bien $\Phi_{n,k} = \sigma(\Phi_{n,\mathbb{Q}})$. □

Pour la suite, on notera simplement Φ_n à la place de $\Phi_{n,K}$.

Proposition 17. Le polynôme Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.

Démonstration. Soit K le corps de décomposition de Φ_n sur $\mathbb{Q}$ et $\zeta \in K$ une racine primitive n-ème de l'unité. On se donne un nombre premier p ne divisant pas n.

Le choix de p implique que ζ^p est une autre racine primitive de l'unité. En effet les autres racines n-ème de l'unité sont de la forme ζ^m avec $\mathrm{pgcd}(m, p) = 1$. Soit F (resp G) le polynôme minimal de ζ (resp ζ^p) sur $\mathbb{Q}$. Alors on a $F, G \in \mathbb{Z}[X]$. En effet comme $\mathbb{Z}[X]$ est factoriel on a $\Phi_n = F_1^{a_1}...F_r^{a_r}$ avec $F_i \in \mathbb{Z}[X]$ irréductible. Comme Φ_n est unitaire il en est de même des F_i (quitte à multiplier les F_i par -1). Mais alors, ζ est racine de l'un des F_i. Comme F_i est unitaire et irréductible que $\mathbb{Q}$, ce ne peut être que F. De même pour G. Notons que F et G divisent Φ_n dans $\mathbb{Z}[X]$. Montrons qu'on a $F = G$. Sinon, comme F et G sont irréductibles et distincts, le produit FG divise Φ_n dans $\mathbb{Z}[X]$. Par ailleurs comme $G(\zeta^p) = 0$, ζ est racine du polynôme $G(X^p)$, donc F divise $G(X^P)$ a priori dans $\mathbb{Q}[X]$ mais aussi dans $\mathbb{Z}[X]$: $G(X^p) = F(X)H(X)$ avec $H \in \mathbb{Z}[X]$. (Si $H \in \mathbb{Q}[X]$, on l'écrit $H = \frac{a}{b}H'$ avec $H' \in \mathbb{Z}[X]$ et on utilise le Lemme de Gauss.) En passant à $\mathbb{F}_p$ on obtient $G(X) = a_rX^r + ... + a_0$ avec $a_i \in \mathbb{Z}$ d'où $g(X^p) = a_rX^{pr} + ... + a_1X^p + a_0$, mais modulo p on a $\overline{a_i} = \overline{a_i}^p$ (par Frobenius)

$$\overline{G}(X^p) = (\overline{a_r}X^r + ... + \overline{a_0})^p = \overline{G}(X)^p$$

Soit alors φ un facteur irréductible de $\overline{F}$ sur $\mathbb{F}_p$. On a $\overline{G}(X)^p = \overline{F}(X)\overline{H}(X)$ et donc φ divise $\overline{G}$. Comme FG divise φ sur n, $\overline{FG}$ divise $\overline{\Phi}_n$ sur $\mathbb{F}_p$ donc φ^2 divise $\overline{\Phi}_n = \Phi_{n,\mathbb{F}_p}$. Mais alors $\Phi_{n,\mathbb{F}_p}$ admet une racine double dans une clôture algébrique de $\mathbb{F}_p$, ce qui est impossible car p ne divise pas n.

Si ζ' est une autre racine primitive n-ème, $\zeta' = \zeta^m$ avec $m = p_1^{a_1}...p_r^{a_R}$ et les p_i sont premiers à n, on a que ζ et ζ' ont aussi le même polynôme irréductible sur $\mathbb{Q}$. On a donc $F(\zeta') = 0$ de sorte que F admet toutes les racines primitives de l'unité comme zéros. On a donc $\deg(F) \geq \varphi_n$ et comme $f|\Phi_n$ cela impose $f = \Phi_n$. Il en résulte que Φ_n est irréductible que $\mathbb{Q}$ et donc sur $\mathbb{Z}$ puisque Φ_n est unitaire. □

Proposition 18. Soit ω une racine primitive n-ème de l'unité. L'extension $\mathbb{Q}(\omega)/\mathbb{Q}$ est galoisienne de groupe de Galois isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$.

Démonstration. Les conjugués de ω sont de la forme ω^k et sont donc tous dans $\mathbb{Q}(\omega)$. L'extension $\mathbb{Q}(\omega)/\mathbb{Q}$ est donc normale puis galoisienne. Pour tout couple d'entiers (h, k) de $\mathbb{Z}$ on a

$$\omega^h = \omega^k \Leftrightarrow h \equiv k \mod n.$$

La notation ω^α avec $\alpha \in \mathbb{Z}/n\mathbb{Z}$ a donc un sens. Les conjugués de ω dans Ω sont les racines primitive n-ème de 1, i.e., les ω^α avec $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$. Un $\mathbb{Q}$-automorphisme σ de $\mathbb{Q}(\omega)$ est entièrement déterminé par l'image $\sigma(\omega) = \omega^\alpha$ avec $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$. Pour $\alpha, \beta \in (\mathbb{Z}/n\mathbb{Z})^*$, on a

$$(\sigma_\beta \circ \sigma_\alpha)(\omega) = \sigma_\beta(\omega^\alpha) = (\sigma_\beta(\omega))^\alpha = (\omega^\beta)^\alpha = \omega^{\beta\alpha} = \sigma_{\beta\alpha}(\omega).$$

On a donc $\sigma_\beta \circ \sigma_\alpha = \sigma_{\beta\alpha}$. L'application

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^* & \to & \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \\ \alpha & \mapsto & \sigma_\alpha \end{array}$$

est alors un isomorphisme de groupe. □