

Corps des racines

1 Introduction

Tous les corps considérés dans ce cours seront des corps commutatifs. Soit K un tel corps.

Définition On dit qu'un corps E est une **extension** du corps K si, et seulement si, K est un sous-corps de E .

Exemple \mathbb{C} est une extension de \mathbb{R} et de \mathbb{Q} .

Exemple \mathbb{R} est une extension de $\mathbb{Q}(\sqrt{2})$.

Exemple $\mathbb{Q}(\sqrt{2})$ est une extension de \mathbb{Q} .

Exemple Le corps $K(X)$ des fractions rationnelles à une indéterminée sur le corps K est une extension de K .

Définition On appelle **équation polynomiale** sur K toute équation de la forme $P(x) = 0$, où P est polynôme appartenant à $K[X]$.

Le **degré** de cette équation est le degré du polynôme. Les **solutions** de cette équation $P(x) = 0$ sont les racines du polynôme P dans une extension E de K .

Exemple Une équation de degré 1 est de la forme $ax + b = 0$ où $a \in K^*$ et $b \in K$.

Exemple Une équation de degré 2 est de la forme $ax^2 + bx + c = 0$ où $a \in K^*$, $b \in K$ et $c \in K$.

Le but de ce cours est de répondre aux deux questions suivantes :

Question 1 : Ayant une équation polynomiale de degré n sur un corps K , est-il possible de trouver une extension E de K , dans laquelle, l'équation possède une solution ?

Question 2 : Dans le cas où l'équation polynomiale $P(x) = 0$ possède une solution dans une extension E de K , sous quelles conditions cette solution s'exprime-t-elle, à partir des coefficients de P , à l'aide des quatre opérations et des radicaux ?

2 Corps des racines

Soit K un corps.

Définition une extension E de K est un **corps de rupture** pour le polynôme $f(X) \in K[X]$ sur K si, et seulement si, E contient une racine de f .

Exemple \mathbb{R} est un corps de rupture pour $X^3 - 2$ sur \mathbb{Q} .

Théorème Si $f(X)$ est un polynôme irréductible dans $K[X]$, alors f possède un corps de rupture sur K .

Démonstration Soit M l'idéal de $K[X]$ engendré par le polynôme f . M est un idéal maximal car $K[X]$ est un anneau principal et f est irréductible. Si E désigne l'anneau quotient $K[X]/M$, alors E est un corps. On peut regarder K comme un sous-corps de E .
 Pour voir ça, soit $p: K[X] \rightarrow K[X]/M$ la surjection canonique. La restriction q de p à K est un homomorphisme non nul car $p(1) = \bar{1}$. Il en résulte que cet homomorphisme est injectif car son anneau de départ est un corps. On en déduit que K est isomorphe à $q(K)$, ce qui permet d'identifier K et $q(K)$. Ainsi E devient une extension de K . Soit $\alpha = \bar{X} = p(X)$. En écrivant

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

nous obtenons

$$\begin{aligned} f(\alpha) &= a_0 + a_1\alpha + \cdots + a_n\alpha^n \\ &= q(a_0) + q(a_1)p(X) + \cdots + q(a_n)(p(X))^n \\ &= p(a_0) + p(a_1)p(X) + \cdots + p(a_n)(p(X))^n \\ &= p(a_0 + a_1X + \cdots + a_nX^n) \\ &= p(f) \\ &= \bar{0} \end{aligned}$$

Donc E est une extension de K contenant la racine α de f .

Corollaire Tout polynôme $f(X) \in K[X]$ possède un corps de rupture sur K .

Démonstration En effet, tout polynôme $f \in K[X]$ se décompose en produit de polynômes irréductibles.

Définition Une extension E de K est un **corps de décomposition** pour un polynôme f sur K si, et seulement si, f peut être scindé dans $E[X]$ c.d. il peut être décomposé en produit de polynômes linéaires dans $E[X]$.

Exemple Le corps \mathbb{C} est un corps de décomposition sur \mathbb{R} pour le polynôme $X^2 + 1$.

Exemple Le corps \mathbb{Q} est un corps de décomposition sur \mathbb{Q} pour le polynôme $X^2 - 1$.

Théorème Tout polynôme $f \in K[X]$ possède un corps de décomposition sur K .

Démonstration On procède par récurrence sur le degré n de f . Si $n = 1$, alors K est un corps de décomposition pour f sur K . Supposons le théorème vrai pour tout polynôme de degré plus petit que n et démontrons-le pour les polynômes de degré n . D'après le corollaire précédent, il existe une extension E de K contenant une racine a de f . Le polynôme $X - a$ divise $f(X)$ dans $E[X]$. Nous avons $f(X) = (X - a)g(X)$ dans $E[X]$, avec $\deg(g) = n - 1$. L'hypothèse de récurrence nous permet de trouver un corps de décomposition F pour $g(X)$ sur E . On a $g(X) = k \prod_{i=2}^{i=n} (X - a_i)$ dans $F[X]$ et

$$f(X) = (X - a)g(X) = (X - a)k \prod_{i=2}^{i=n} (X - a_i) = k \prod_{i=1}^{i=n} (X - a_i)$$

dans $F[X]$ où $a_1 = a$. Ainsi, F est un corps de décomposition pour f sur K .

Définition Un corps de décomposition minimal pour f sur K est appelé un **corps des racines** pour f sur K .

Exemple \mathbb{C} est un corps des racines sur \mathbb{R} pour le polynôme $X^2 + 1$.

Exemple $\mathbb{Q}(\sqrt{2})$ est un corps de décomposition sur \mathbb{Q} pour le polynôme $X^2 - 2$.

3 Adjonction

Définition Soit A est une partie d'une extension E de K . Le sous-corps de E engendré par $K \cup A$ est appelé le **corps engendré par A sur K** ou le corps obtenu par l'**adjonction** de A à K . On dira alors que A est un **système de générateurs** de $K(A)$ sur K .

Notation Le corps engendré par A sur K sera désigné par $K(A)$. Si A est fini et si a_1, \dots, a_n sont ses éléments, alors nous écrirons $K(a_1, \dots, a_n)$ à la place de $K(A)$.

Exemple Si $A = \emptyset$, alors $K(A) = K$.

Exemple $\mathbb{C} = \mathbb{R}(i)$.

Remarque Une extension E de K peut avoir plusieurs système de générateurs sur K : ainsi $\mathbb{R}(i) = \mathbb{C} = \mathbb{R}(1 + i)$.

Théorème Si A et B sont deux parties d'une extension E de K , alors $K(A \cup B) = K(A)(B)$.

Démonstration Tout sous-corps de E qui contient K, A et B contient $K(A)$ et B . Réciproquement, tout sous-corps de E qui contient $K(A)$ et B contient K, A et B . Il en résulte que la famille de tous les sous-corps de E contenant K, A et B est égale à celle de tous les sous-corps de E qui contiennent $K(A)$ et B . Ceci prouve que $K(A \cup B)$, qui est le plus petit élément de la première famille, est égal à $K(A)(B)$, qui est le plus petit élément de la seconde.

Corollaire $K(a_1, \dots, a_n) = K(a_1, \dots, a_{n-1})(a_n)$.

Théorème Tout polynôme $f \in K[X]$, possède un corps des racines sur K .

Démonstration Soit E un corps de décomposition pour f sur K . Ce polynôme s'écrit sous la forme

$$f(X) = k \prod_{i=1}^{i=n} (X - a_i)$$

dans $E[X]$. Soit $S = K(a_1, \dots, a_n)$. Il est facile de voir que S est un corps de décomposition pour f sur K . Ce corps de décomposition est minimal car, si R est un corps de décomposition pour f sur K contenu dans S , alors f s'écrit

$$f(X) = k' \prod_{i=1}^{i=n} (X - b_i)$$

dans $R[X]$. Mais $R[X] \subseteq S[X]$. Il en résulte que f s'écrit de deux manières comme produit de polynômes linéaires qui sont irréductibles. L'unicité d'une telle décomposition implique $k = k'$ et $\{a_1, \dots, a_n\} = \{b_1, \dots, b_n\}$. D'où

$$R \subseteq S = K(a_1, \dots, a_n) = K(b_1, \dots, b_n) \subseteq R$$

ce qui prouve $R = S$. S est un corps des racines pour f sur K .

Théorème Si E est un corps de décomposition sur K pour le polynôme $f(X) \in K[X]$, alors E contient un corps des racines unique pour f sur K .

Démonstration Si

$$f(X) = k \prod_{i=1}^{i=n} (X - a_i) \in E[X]$$

est la décomposition de f comme produit de facteurs linéaires dans $E[X]$, alors a_1, a_2, \dots, a_n sont les racines de f dans E et $R = K(a_1, a_2, \dots, a_n)$ est un corps des racines pour f sur K comme nous l'avons vu. Si T est un autre corps des racines pour f sur K , alors f s'écrit

$$f(X) = k' \prod_{i=1}^{i=n} (X - b_i) \in T[X]$$

Il en résulte

$$f(X) = k \prod_{i=1}^{i=n} (X - a_i) = k' \prod_{i=1}^{i=n} (X - b_i) \in E[X]$$

L'unicité d'une telle décomposition implique $k = k'$ et

$$\{a_1, \dots, a_n\} = \{b_1, \dots, b_n\}$$

. Ainsi $R \subseteq T$ et $R = T$ car T est un corps de décomposition minimal pour f sur K .

4 Degré d'une extension

Soit E une extension de K . E peut être muni d'une structure de K -espace vectoriel en définissant la multiplication par un scalaire par

$$(\alpha, x) \mapsto \alpha x$$

Définition On appelle **degré** de l'extension E , la dimension de E en tant que K -espace vectoriel. Ce degré sera noté $[E : K]$.

Exemple $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{R} : \mathbb{Q}]$ est infini.

Exemple $[K : K] = 1$.

Définition Une extension E de K sera dite **finie** si, et seulement si, $[E : K]$ est fini. Elle sera dite **infinie** dans le cas contraire.

Théorème de la multiplicativité du degré Si E est une extension de K et L est un corps intermédiaire entre K et L , alors

$$[E : K] = [E : L][L : K].$$

Démonstration Soit $(x_i)_{i \in I}$ une base du L -espace vectoriel E et $(y_j)_{j \in J}$ une base du K -espace vectoriel L . Nous allons prouver que $(x_i y_j)_{(i,j) \in I \times J}$ est une base du K -espace vectoriel E .

C'est un système de générateurs : tout $x \in E$ s'écrit $x = \sum_{i \in I} a_i x_i$ où $a_i \in L$ pour tout $i \in I$. Or tout a_i peut s'écrire $a_i = \sum_{j \in J} b_{ij} y_j$. Nous obtenons

$$x = \sum_{i \in I} a_i x_i = \sum_{i \in I} \left(\sum_{j \in J} b_{ij} y_j \right) x_i = \sum_{(i,j) \in I \times J} b_{ij} x_i y_j$$

C'est un système libre : Si $\sum_{(i,j) \in I \times J} b_{ij} x_i y_j = 0$ alors

$$\sum_{i \in I} \left(\sum_{j \in J} b_{ij} y_j \right) x_i = 0$$

ce qui implique $\sum_{j \in J} b_{ij} y_j = 0$ pour tout $i \in I$ car $(x_i)_{i \in I}$ est une base du L -espace vectoriel E . Mais $(y_j)_{j \in J}$ est une base du K -espace vectoriel L , d'où $b_{ij} = 0$ pour tout $(i,j) \in I \times J$.

La famille $(x_i y_j)_{(i,j) \in I \times J}$ étant une base du K -espace vectoriel E , nous avons

$$\begin{aligned} [E : K] &= \dim_K(E) = \text{Card}(I \times J) = \text{Card}(I) \times \text{Card}(J) \\ &= \dim_L(E) \times \dim_K(L) = [E : L][L : K]. \end{aligned}$$

Corollaire Si $(E_i)_{i=1, \dots, n}$ est une suite croissante de corps $K = E_0 \subseteq E_1 \subseteq \dots \subseteq E_n = E$ alors

$$[E : K] = [E_n : E_0] = \prod_{i=1}^{i=n} [E_i : E_{i-1}]$$

Démonstration Par une simple récurrence.