Extensions simples

1 Extensions simples

Définition Une extension E de K est **simple** si, et seulement si, il existe $a \in E$ tel que $E = K(a)$.

Exemple $\mathbb{C} = \mathbb{R}(i)$ est une extension simple de $\mathbb{R}$, $K(X)$ est une extension simple de K.

L'importance des extensions simples provient du fait que leurs structures peuvent être parfaitement déterminées d'une part et que la majorité des extensions que nous allons rencontrer sont en réalité des extensions simples. Nous allons déterminer la structure d'une extension simple.

Théorème Soit $E = K(a)$ une extension de K. Il existe un homomorphisme d'anneaux et un seul

$$\sigma; K[X] \longrightarrow E$$

qui vérifie $\sigma(X) = a$ et $\sigma(k) = k$ pour tout $k \in K$.

Démonstration Soit $\sigma; K[X] \longrightarrow E$ l'application définie par $\sigma(P) = P(a)$ pour tout $P \in K[X]$. Il est facile de vérifier que σ satisfait les conditions du théorème. Il nous reste à prouver l'unicité de σ. Si τ est une autre solution, alors nous avons pour tout $P = \sum_{i=0}^{i=n} b_i X^i$ dans $K[X]$

$$\tau(P) = \tau\left(\sum_{i=0}^{i=n} b_i X^i\right) = \sum_{i=0}^{i=n} \tau(b_i)\,\tau(X)^i = \sum_{i=0}^{i=n} b_i a^i = P(a) = \sigma(P)$$

D'où $\tau = \sigma$.

Définition - Notation Le sous-anneau de E engendré par $K \cup \{a\}$ sera noté $K[a]$ alors que $K(a)$ désigne le sous-corps de E engendré $K \cup \{a\}$.

Théorème $\mathrm{Im}(\sigma)$ est le sous-anneau $K[a]$ de E engendré par $K \cup \{a\}$.

Démonstration $\mathrm{Im}(\sigma)$ est un sous-anneau de E. Il contient $K = \sigma(K)$ et $a = \sigma(X)$. Si L est un sous-anneau de E contenant $K \cup \{a\}$ alors $\mathrm{Im}(\sigma) \subseteq L$ car tout élément c de $\mathrm{Im}(\sigma)$ s'écrit $c = P(a) = \sum_{i=0}^{i=n} b_i a^i \in L$.

Définition Soit $\sigma; K[X] \longrightarrow E$ l'application définie par $\sigma(P) = P(a)$ pour tout $P \in K[X]$. Considérons le noyau de σ. C'est un idéal de $K[X]$.

Deux cas sont possibles : $Ker(\sigma) = (0)$ ou $Ker(\sigma) \neq (0)$. Dans le premier cas, l'élément a de E sera dit **transcendant** sur K, et dans le second, a sera dit **algébrique** sur K.

Exemple $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ alors que π est transcendant sur $\mathbb{Q}$.

Exemple $X \in K(X)$ est transcendant sur K.

1.1 Cas où a est algébrique sur K

$I(a) = Ker(\sigma)$, est un idéal non nul de $K[X]$. Mais $K[X]$ est un anneau principal. Donc $Ker(\sigma)$ est principal. D'un autre côté, deux générateurs de $I(a)$ sont tels que l'un d'eux est le produit de l'autre par un élément de K^*, il en résulte que cet idéal possède un générateur unitaire et un seul.

Définition Le générateur unitaire de $I(a) = Ker(\sigma)$ sera noté $Irr(a,K)$ et appelé le **polynôme minimal** de a sur K.

Exemple i est algébrique sur $\mathbb{R}$ et $Irr(i,\mathbb{R}) = X^2 + 1$.

Exemple $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ et $Irr(i,\mathbb{Q}) = X^2 - 2$.

Théorème Le polynôme $Irr(a,K)$ est irréductible dans $K[X]$.

Démonstration Sinon, on pourra l'écrire sous la forme $Irr(a,K) = gh$ où g et h sont deux polynômes de degré inférieur au degré n de $Irr(a,K)$. Mais, nous avons

$$g(a)\,h(a) = (gh)(a) = Irr(a,K)(a) = 0$$

qui implique $g(a) = 0$ ou $h(a) = 0$. Dans le premier cas, nous aurons $g \in I(a)$ et $Irr(a,K)$ divise g, et dans le second cas, $h \in I(a)$ et $Irr(a,K)$ divise h ce qui est impossible vu les degrés de ces polynômes.

Remarque Nous avons

$$[f(a) = 0] \Longleftrightarrow [f \in I(a)] \Longleftrightarrow [Irr(a,K) \text{ divise } f]$$

Le théorème précédent justifie la notation $Irr(a,K)$ pour le polynôme minimal de a sur K.

Théorème
Soient L et E des extensions du corps K. Si $K \subseteq L \subseteq E = K(a)$, alors $E = L(a)$ et $Irr(a,L)$ divise $Irr(a,K)$ dans $L[X]$.

Démonstration E est un sous-corps de E contenant $L\cup\{a\}$. Si H est un sous-corps de E contenant $L\cup\{a\}$, alors H contient $K\cup\{a\}$ et $E\subseteq H$ car E est le plus petit sous-corps de E contenant $K\cup\{a\}$. Donc E est le plus petit sous-corps de E contenant $L\cup\{a\}$, ce qui prouve $E=L(a)$. Le polynôme $Irr(a,K)$ appartient à $L[X]$ et vérifie $Irr(a,K)(a)=0$. Il en résulte que $Irr(a,L)$ divise $Irr(a,K)$ dans $L[X]$.

Théorème Si a est algébrique sur K, alors

$$K(a)=K[a]\approx K[X]/I(a)$$

où $I(a)=\{P(a);P\in K[X]\}$.

Démonstration Considérons l'homomorphisme σ défini par $\sigma(P)=P(a)$ pour tout $P\in K[X]$. Nous avons

$$K[a]=\mathrm{Im}(\sigma)\approx K[X]/Ker(\sigma)\approx K[X]/I(a).$$

Il en résulte que $K[a]$ est un corps car l'idéal $I(a)$ est maximal. Ceci prouve $K(a)=K[a]$ et par suite $K(a)=K[a]\approx K[X]/I(a)$.

Théorème Soit a algébrique sur le corps k. Si $n=deg(Irr(a,K))$, alors $E=K(a)$ est une extension de degré n et $\left\{1,a,a^2,...,a^{n-1}\right\}$ est une base du K-espace vectoriel E.

Démonstration Les éléments $1,a,a^2,...,a^{n-1}$ sont linéairement indépendants car sinon, on peut trouver un polynôme non nul de degré inférieur ou égal à $n-1$ dont a est une racine. Ce polynôme appartiendrait à $I(a)$ ce qui est impossible car $I(a)$ est engendré par un polynôme de degré n. Pour prouver que ces éléments forment un système de générateurs du K-espace vectoriel E, il suffit de démontrer que

$$a^m\in Vect\left(1,a,a^2,...,a^{n-1}\right)$$

pour tout $m\in\mathbb{N}$ car tout élément de $K(a)=K[a]$ s'écrit sous la forme $x=\alpha_0+\alpha_1a+\cdots+\alpha_qa^q$. Ceci est vrai pour $m\leq n-1$. Si $m\geq n$, alors m s'écrit $m=n+r$. Nous allons démontrer $a^m\in Vect\left(1,a,a^2,...,a^{n-1}\right)$ par récurrence sur r. Si $r=0$, alors $m=n$. En écrivant $Irr(a,K)$ sous la forme

$$Irr(a,K)=b_0+b_1X+\cdots+b_{n-1}X^{n-1}+X^n,$$

on obtient

$$b_0+b_1a+\cdots+b_{n-1}a^{n-1}+a^n=0$$

et

$$a^n=c_0+c_1a+\cdots+c_{n-1}a^{n-1}\in Vect\left(1,a,a^2,...,a^{n-1}\right)$$

où $c_i=-b_i$ pour $1=0,1,...,n-1$.

Supposons que

$$a^{n+r}=t_0+t_1a+\cdots+t_{n-1}a^{n-1}\in Vect\left(1,a,a^2,...,a^{n-1}\right)$$

alors nous avons

$$a^{n+r+1} = aa^{n+r} = at_0 + t_1a^2 + \cdots + t_{n-1}a^n \in Vect\left(1,a,a^2,...,a^{n-1}\right)$$

car

$$at_0 + t_1a^2 + \cdots + t_{n-2}a^{n-1} \in Vect\left(1,a,a^2,...,a^{n-1}\right)$$

et

$$t_{n-1}a^n \in Vect\left(1,a,a^2,...,a^{n-1}\right)$$

Il en résulte $a^m \in Vect\left(1,a,a^2,...,a^{n-1}\right)$ pour tout $m \in \mathbb{N}$. Ceci prouve $[E:K] = \dim_K(E) = n$.

1.2 Cas où a est transcendant sur K

Dans ce cas, l'homomorphisme σ est injectif. Ceci prouve que $K[X]$ est isomorphe à $K[a]$. Mais ces deux anneaux possèdent des corps de fractions, et σ peut être prolongé en un homomorphisme du corps de fractions $Q(K[X]) = K(X)$ de $K[X]$ au corps de fractions $Q(K[a]) = K(a) = E$ de $K[a]$. Il en résulte :

Théorème
ancc1 Si a est transcendant sur K, alors $E = K(a)$ est isomorphe à $K(X)$.

2 Extensions algébriques

Définition Une extension E d'un corps K sera dite **algébrique** si, et seulement si, tout élément a de E est algébrique sur K. Elle sera dite **transcendante** dans le cas contraire.

Exemple $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$, mais $\mathbb{R}$ est une extension transcendante de $\mathbb{Q}$.

Théorème Toute extension finie E d'un corps K est algébrique.

Démonstration Soit a un élément de E et $n = [E:K]$. Les éléments $1,a,a^2,...,a^n$ sont linéairement dépendants car $\dim_K(E) = n$. Il existe des scalaires (éléments de K) $b_0,b_1,...,b_n$, non tous nuls, tels que

$$b_0 + b_1a + \cdots + b_{n-1}a^{n-1} + b_na^n = 0.$$

Si

$$P = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} + b_nX^n,$$

alors $P \neq 0$ et $P(a) = 0$ ce qui prouve que a est algébrique sur K. Il en résulte que E est une extension algébrique de K.

Théorème Une extension simple $E = K(a)$ est algébrique si, et seulement si, a est algébrique sur K.

Démonstration Si a est algébrique sur K, alors E est une extension finie de K ce qui prouve que cette extension est algébrique. Réciproquement, si l'extension E est algébrique, alors a, élément de E, est algébrique sur K.

Théorème Si $K \subseteq L \subseteq E$, alors si $a \in E$ est algébrique sur K, alors il est algébrique sur L.

Démonstration Si a est algébrique sur K, alors a est une racine d'un polynôme $f \in K[X]$. Mais $f \in L[X]$ car $K \subseteq L$. Il en résulte que a est algébrique sur L.

Théorème L'extension $E = K(a_1,a_2,...,a_n)$ de K est algébrique si, et seulement si, les éléments $a_1,a_2,...,a_n$ sont tous algébriques sur K.

Démonstration Si E algébrique sur K, alors les éléments $a_1,a_2,...,a_n$ de E sont tous algébriques sur K. Réciproquement, nous allons démontrer que si les éléments $a_1,a_2,...,a_n$ sont tous algébriques sur K, alors l'extension E de K est finie. Posons

$$K_0 = K \text{ et } K_i = K(a_1,a_2,...,a_i) \text{ pour } i = 1,2,..,n$$

Nous avons $K_i = K_{i-1}(a_i)$. D'un autre côté, a_i est algébrique sur K_{i-1} car a_i est algébrique sur K et $K \subseteq K_{i-1} \subseteq K_i$. Ceci implique que le degré $[K_i : K_{i-1}]$ est fini pour tout i et $[E : K] = [K_n : K_0] = \prod_{i=1}^{i=n} [K_i : K_{i-1}]$ est fini. Ainsi, l'extension E de K est finie. Elle est algébrique.

Corollaire Si R est un corps des racines pour $P(X) \in K[X]$ sur K, alors R est une extension algébrique de K.

Démonstration Nous avons $R = K(a_1,a_2,...,a_n)$ où $a_1,a_2,...,a_n$ sont les racines de P dans R. Comme chaque a_i est algébrique sur K (il est racine de P), R est une extension algébrique de K.

3 Simplicité d'une extension

Le but de ce paragraphe est de prouver qu'une extension finie E de K est simple si, et seulement si, l'ensemble des corps inermédiaires entre K et E est fini. Ceci découlera des théorèmes suivants :

Théorème Si $E = K(a)$, où a est algébrique sur K, et si L est un corps intermédiaire entre K et E, alors $Irr(a,L)$ divise $Irr(a,K)$ et $L = K(a_1,a_2,...,a_{n-1})$ où $a_1,a_2,...,a_{n-1}$ sont les coéfficients de $Irr(a,L)$.

Démonstration Soit $H = K(a_1,a_2,...,a_{n-1})$. Nous avons

$$K \subseteq H \subseteq L \subseteq E = K(a).$$

$Irr(a,L)$ appartient à $H[X]$ et est irréductible dans $H[X]$ car il est irréductible dans $L[X]$ ($H[X] \subseteq L[X]$). Il en résulte

$$Irr(a,H) = irr(a,L) \text{ et } H(a) = E = L(a).$$

Ce qui précède implique

$$[E:H] = \deg(Irr(a,H)) = \deg(Irr(a,L)) = [E:L]$$

et

$$[L:H] = \frac{[E:H]}{[E:L]} = 1.$$

D'où $H = L$.

Théorème Si $E = K(a)$ est une extension simple, alors l'ensemble des corps intermédiaires entre K et E est fini.

Démonstration Soit φ l'application de l'ensemble des corps intermédiaires dans celui des facteurs de $Irr(a,K)$ qui associe à L le facteur $Irr(a,L)$. Cette application est injective, car si $Irr(a,L) = Irr(a,L')$, alors L et L' sont tous les deux égaux au corps engendré sur K par les coefficients du polynôme $Irr(a,L) = Irr(a,L')$. On en déduit que l'ensemble des corps intermédiaires est fini car l'ensemble des facteurs de $Irr(a,K)$ est fini.

Pour prouver la réciproque, nous distingons deux cas :_

3.1 Cas où K est fini

Théorème Si K est un corps fini et E est une extension finie de K, alors E est une extension simple de K.

Démonstration Si $Card(K) = q$ et $[E:K] = n$, alors $Card(E) = q^n$ car le K-espace vectoriel E est isomorphe à K^n. Il en résulte que E est un corps fini. Nous prouverons par la suite que le groupe multiplicatif d'un corps fini est cyclique. On en déduit que si a est un générateur du groupe E^*, alors $E = K(a)$.

3.2 Cas où K est infini

Théorème Si l'ensemble des corps intermédiaires entre K et E est fini et si $E = K(a_1,a_2)$, alors E est une extension simple de K.

Démonstration Considérons l'ensemble des corps intermédiaires de la forme $K(a_1+ta_2)$ où $t \in K$. Cet ensemble est fini. Comme K est infini, il existe deux éléments distincts t et u tels que

$$K(a_1+ta_2) = K(a_1+ua_2) = L$$

. Nous avons

$$(t-u)a_2 = (a_1+ta_2) - (a_1+ua_2) \in L$$

et $a_2 \in L$ car $t-u \neq 0$. Nous avons aussi $a_1 = (a_1+ta_2) - ta_2 \in L$. Il en résulte

$$L = K(a_1+ta_2) = K(a_1,a_2) = E.$$

Théorème Toute extension finie E de K est engendrée sur K par un nombre fini d'éléments c.à.d. elle est de la forme $E = K(a_1,a_2,...,a_n)$.

Démonstration Nous allons démontrer ce théorème par récurrence sur le degré $p = [E:K]$. Si $p = 2$ et $a \in E-K$, alors $K \neq K(a) \subseteq E$ et

$$1 < [K(a):K] \leq [E:K] = 2.$$

Il en résulte $[K(a):K] = [E:K] = 2$ et $E = K(a)$. Si le théorème est vrai pour les extensions de degrés $\leq p-1$, il est aussi vrai pour les extensions de degré p. En effet, si $a_1 \in E-K$, alors $[E:K(a_1)] \leq p-1$. Il en résulte que E s'écrit $E = K(a_1)(a_2,...,a_n) = K(a_1,...,a_n)$.

Théorème Si l'ensemble des corps intermédiaires entre K et E est fini, alors E est une extension simple de K.

Démonstration Comme E est une extension finie de K, E est de la forme

$$E = K(a_1,a_2,...,a_n).$$

Nous allons prouver le théorème par récurrence sur n. Pour $n = 2$, le théorème est vrai comme nous l'avons démontré ci-haut. Supposons le théorème vrai pour $n-1$. L'extension $E = K(a_1,a_2,...,a_{n-1})$ est telle que l'ensemble des corps intermédiaires est fini. C'est donc une extension simple $K(b)$ de K. Nous obtenons

$$E = K(a_1,a_2,...,a_n) = K(a_1,a_2,...,a_{n-1})(a_n) = K(b,a_1).$$

Mais cette extension est simple d'après ce qui a été démontré. Donc E est une extension simple de K.

Théorème Une extension finie E de K est simple si, seulement si, l'ensemble des corps intermédiaires entre K et E est fini.

Exemple $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$.

Définition On appelle **élément primitif** d'une extension finie E de K, tout élément a de E tel que $E = K(a)$.

Exemple i est un élément primitif de l'extension $\mathbb{C}$ de $\mathbb{R}$. $\sqrt{2}+\sqrt{3}$ est un élément primitif de l'extension $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ de $\mathbb{Q}$.