Extensions séparables

1 Degré de Galois d'une extension

Toutes les extensions considérées dans ce chapitre **seront finies**. Soit E une extension de K, N et N' deux clôtures normales de E, I l'ensemble des K-isomorphismes de E dans N et I' celui des K-isomorphismes de E dans N'.

Théorème $Card(I) = Card(I')$.

Démonstration N et N' sont deux clôtures normales de E. Il existe un K-isomorphisme σ de N sur N'. Soit $\varphi; I \longrightarrow I'$ l'application définie par $\varphi(u) = \sigma \circ u$. Il est facile de prouver que l'application φ est bijective. Donc $Card(I) = Card(I\prime)$.

Définition On appelle **degré galoisien** d'une extension E de K, le cardinal de l'ensemble des K-isomorphismes de E dans une clôture normale de E.
La définition du degré galoisien ne dépend pas du choix de la clôture normale de E d'après le théorème précédent. Le degré galoisien de l'extension E de K sera noté $\overline{[E:K]}$.

Exemple $\overline{[\mathbb{C}:\mathbb{R}]} = 2$.

Théorème Soit L une extension normale de K contenant une clôture normale de E. Le degré galoisien $\overline{[E:K]}$ est égal au cardinal de l'ensemble des K-isomorphismes de E dans L.

Démonstration Soit J l'ensemble des K-isomorphismes de E dans L. Nous avons $I \subseteq J$. Réciproquement, tout $\sigma \in J$ peut être prolongé en un K-automorphisme $\overline{\sigma}$ de L, car L est une extension normale de K. La restriction de $\overline{\sigma}$ à N est un K-automorphisme de N car N est une extension normale de K. Nous avons $\sigma(E) \subseteq \overline{\sigma}(E) \subseteq \overline{\sigma}(N) = N$. Il en résulte que, σ est, en réalité, un K-isomorphisme de E dans N c.à.d. $\sigma \in I$. D'où $I = J$.

Théorème Soit E' une extension de K'. Si $\overline{\sigma}$ est un isomorphisme de E sur E' tel que sa restriction σ à K est un isomorphisme de K sur K', alors $\overline{[E:K]} = \overline{[E':K']}$.

Démonstration Soit N une clôture normale de E et N' une clôture normale de E'. L'isomorphisme $\overline{\sigma}$ peut être prolongé en un isomorphisme σ' de N sur N'. L'application φ qui associe à chaque K-isomorphisme u de E dans N, le K'-isomorphisme $u' = \sigma \circ u \circ \sigma^{-1}$ de E' dans N' est bijective. Il en résulte $\overline{[E:K]} = \overline{[E':K']}$.

Théorème Si nous avons $K \subseteq L \subseteq E$, alors $\overline{[E:K]} = \overline{[E:L]} \times \overline{[L:K]}$.

Démonstration Soit N une clôture normale de E. Pour tout K-isomorphisme σ

de L dans N, on note J_σ l'ensemble de tous les K-isomorphismes de E dans N qui prolongent σ. Si $\overline{\sigma} \in J_\sigma$, alors $\overline{\sigma}(E)$ est un corps intermédiaire entre $\sigma(L)$ et N. Soit I_σ l'ensemble des tous les $\sigma(L)$-isomorphismes de $\overline{\sigma}(E)$ dans N. Nous allons prouver que I_σ et J_σ ont le même cardinal. Considérons l'application $f; I_\sigma \longrightarrow J_\sigma$ définie par $f(u) = u \circ \overline{\sigma}$. Il est facile de voir que f est injective. Elle est aussi surjective; car si $u' \in J_\sigma$, u' peut s'écrire sous la forme $u' = f\left(u' \circ \overline{\sigma}^{-1}\right)$, car $\overline{\sigma}$ peut être regardé comme un isomorphisme de E sur $\overline{\sigma}(E)$. Or, nous avons $Card(I_\sigma) = \overline{[\overline{\sigma}(E) : \sigma(L)]}$ et, d'après le théorème précédent, $\overline{[\overline{\sigma}(E) : \sigma(L)]} = \overline{[E : L]}$. D'où $Card(I_\sigma) = \overline{[E : L]}$. Pour terminer la démonstration, remarquons que (J_σ) est une partition de l'ensemble J des tous les K-isomorphismes de E dans N. Ainsi, nous avons

$$\begin{aligned}\overline{[E : K]} &= Card(J) = \sum_\sigma Card(J_\sigma) = \sum_\sigma Card(I_\sigma) \\ &= \sum_\sigma \overline{[E : L]} = \overline{[E : L]} \times \overline{[L : K]}\end{aligned}$$

Théorème Si $E = K(a)$, alors $\overline{[E : K]}$ est le nombre des racines distinctes de $Irr(a,K)$.

Démonstration Soit N une clôture normale de E, I l'ensemble des tous les K-isomorphismes de E dans N et A l'ensemble des racines distinctes de $Irr(a,K)$ dans N. L'application de I dans A qui associe σ à $\sigma(a)$ est bijective. D'où $\overline{[E : K]} = Card(I) = Card(A)$.

Corollaire Si $E = K(a)$, alors $\overline{[E : K]} \leq [E : K]$.

Théorème Si E est une extension finie de K, alors $\overline{[E : K]} \leq [E : K]$.

Démonstration Comme E est une extension finie de K, elle s'écrit $E = K(a_1,...,a_n)$. Si $K_i = K(a_1,...,a_i)$, alors $K_i = K_{i-1}(a_i)$. Démontrons par récurrence sur i que $\overline{[K_i : K]} \leq [K_i : K]$. Pour $i = 1$, la propriété est vraie car nous avons

$$\overline{[K_1 : K]} = \overline{[K(a_1) : K]} \leq [K(a_1) : K] = [K_1 : K]$$

Supposons le propriété vraie pour i et démontrons-la pour $i+1$. Nous avons

$$\overline{[K_{i+1} : K]} = \overline{[K_{i+1} : K_i]} \times \overline{[K_i : K]} \leq [K_{i+1} : K_i] \times [K_i : K] = [K_{i+1} : K]$$

Par récurrence, nous obtenons

$$\overline{[E : K]} = \overline{[K_n : K]} \leq [K_n : K] = [E : K]$$

2 Extensions Séparables

Soit E une extension of K.

Définition L'extension E de K sera dite **séparable** si, et seulement si, $\overline{[E:K]} = [E:K]$.

Exemple $\mathbb{C}$ est une extension séparable de $\mathbb{R}$.

Définition Un élément a d'une extension E de K sera dit séparable sur K si, et seulement si, toutes les racines de $Irr(a,K)$ sont simples.

Exemple i est séparable sur $\mathbb{R}$. $\sqrt{2}$ séparable sur $\mathbb{Q}$.

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

Démonstration Soit $[E:K] = n = \deg(Irr(a,k))$. Nous avons

$$\begin{aligned}[E \text{ est séparable sur } K] &\Longleftrightarrow \left[\overline{[E:K]} = [E:K]\right] \\ &\Longleftrightarrow [Irr(a,K) \text{ possède } n \text{ racines distinctes}] \\ &\Longleftrightarrow [\text{toute racine de } Irr(a,K) \text{ est simple}] \\ &\Longleftrightarrow [a \text{ est séparable sur } K]\end{aligned}$$

Théorème Une extension finie E de K est séparable si, et seulement si, tout élément a de E est séparable sur K.

Démonstration Si E est séparable sur K, Alors nous avons

$$\begin{aligned}\overline{[E:K(a)]} \times \overline{[K(a):K]} &= \overline{[E:K]} = [E:K] \\ &= [E:K(a)] \times [K(a):K]\end{aligned}$$

Or

$$\overline{[E:K(a)]} \leq [E:K(a)] \text{ et } \overline{[K(a):K]} \leq [K(a):K]$$

D'où

$$\overline{[E:K(a)]} = [E:K(a)] \text{ et } \overline{[K(a):K]} = [K(a):K]$$

et a est séparable sur K. Réciproquement, E s'écrit $E = K(a_1,...,a_n)$ car elle est une extension finie de K. Posons $K_i = K(a_1,...,a_i)$. Nous avons $K_i = K_{i-1}(a_i)$, $Irr(a_i,K_{i-1})$ divise $Irr(a_i,K)$ et a_i est séparable sur K. Il en résulte que a_i est séparable sur K_{i-1} et $\overline{[K_i:K_{i-1}]} = [K_i:K_{i-1}]$ pour $i = 1,2,...,n$. Il en résulte

$$\overline{[E:K]} = \prod_{i=1}^{i=n} [K_i:K_{i-1}] = [E:K]$$

ce qui prouve que E est séparable sur K.

Théorème de l'élément primitif. Toute extension séparable finie E de K est simple.

Démonstration Il suffit de prouver que l'ensemble des corps intermédiaires entre K et E est fini. Soit $\mathcal{F}$ cet ensemble et I l'ensemble des tous les K-isomorphismes de E dans une clôture normale N. Soit $h : \mathcal{F} \longrightarrow P(I)$ l'application qui associe à $L \in \mathcal{F}$ le sous-ensemble de I défini par

$$\{\sigma \in I \quad / \quad \sigma(a) = a \text{ pour tout } a \in L\}.$$

Cette application est injective; car si $L \neq L'$, et si $a \in L - L'$, alors a est séparable sur K, ce qui prouve que a est séparable sur L'. D'où

$$\overline{[L'(a) : L']} = [L'(a) : L'] > 1.$$

Ce qui précède montre qu'il existe un L'-isomorphisme σ de $L'(a)$ dans N tel que $\sigma(a) \neq a$. Or σ peut être prolongé en un K-automorphisme $\overline{\sigma}$ de N car N est une clôture normale. La restriction σ^* de $\overline{\sigma}$ à E est un K-isomorphisme de E dans N qui vérifie $\sigma^*(a) = \overline{\sigma}(a) = \sigma(a) \neq a$. Il en résulte $\sigma^* \in h(L')$ et $\sigma^* \notin h(L)$ qui prouve $h(L) \neq h(L')$. Pour finir la démonstration, notons que l'ensemble $P(I)$ des parties de I est fini car I est fini.