Extensions normales

Soit E une extension algébrique d'un corps K. E peut être un corps de rupture sur K pour un polynôme $f(X) \in K[X]$ sans être un corps de décomposition come le montre l'exemple suivant :

Exemple $\mathbb{R}$ est un corps de rupture pour $X^3 - 2$ sur $\mathbb{Q}$ sans être un corps de décomposition car nous avons :

$$X^3 - 2 = \left(X - \sqrt[3]{2}\right)\left(X^2 + \sqrt[3]{2}X + \sqrt[3]{4}\right)$$

et $X^2 + \sqrt[3]{2}X + \sqrt[3]{4}$ est irréductible dans $\mathbb{R}[X]$.

Définition Une extension algébrique E de K sera dite **normale** si, et seulement si, chaque fois que E est un corps de rupture pour un polynôme irréductible $f(X) \in K[X]$ sur K, il est un corps de décomposition pour f sur K.

Ainsi, E est une extension normale de K si, et seulement si, chaque fois qu'un polynôme irréductible $f(X) \in K[X]$ possède une racine dans E, alors il se décompose en produit de facteurs linéaires dans $E[X]$. Parfois on exprime ceci en disant que E est une extension normale de K si, et seulement si, chaque fois qu'un polynôme irréductible $f(X) \in K[X]$ possède une racine dans E, alors il possède toutes ses racines dans E.

Exemple $\mathbb{C}$ est une extension normale de $\mathbb{R}$ car les polynôme irréductible dans $\mathbb{R}[X]$ sont de degré 1 ou 2.

Exemple L'extension $E = \mathbb{Q}\left(\sqrt[3]{2}\right)$ de $\mathbb{Q}$ n'est pas normale car le polynôme $X^3 - 2 \in \mathbb{Q}[X]$ possède une racine dans E sans se décomposer en produit de facteurs linéaires dans $E[X]$.

Théorème Soit E un corps des racines pour le polynôme $Q(X) \in K[X]$ sur K. Soit $f \in K[X]$ un polynôme irréductible, a et b deux racines de f. Nous avons $[E(a) : E] = [E(b) : E]$.

Démonstration Considérons le diagramme

$$\begin{tikzcd}
E(a) & & E(b) \\
& E \arrow[ul] \arrow[ur] & \\
K(a) \arrow[uu] & & K(b) \arrow[uu] \\
& K \arrow[ul] \arrow[ur] \arrow[uu] &
\end{tikzcd}$$

Si $a_1, \ldots, a_n$ sont les racines de Q dans E, alors nous avons

– $E = K(a_1, \ldots, a_n)$.

– $E(a) = K(a_1,...,a_n,a) = K(a)(a_1,...,a_n)$ est le corps des racines de Q sur $K(a)$.
– $E(b)$ est le corps des racines de Q sur $K(b)$.
– Il existe un K-isomorphisme σ de $K(a)$ sur $K(b)$ tel que $\sigma(a) = b$, car a et b sont deux racines du même polynôme irréductible f (donc $Irr(a,K) = Irr(b,K)$).
– $\widehat{\sigma}(Q) = Q$ car $Q \in K[X]$. Il en résulte que $E(b)$ est le corps des racines de $\widehat{\sigma}(Q)$ sur $K(b)$.
– Le K-isomorphisme σ peut être prolongé en un isomorphisme de $E(a)$ sur $E(b)$.
– On en déduit $[E(a) : K(a)] = [E(b) : K(b)]$ et

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

Théorème Une extension finie E de K est normale si, et seulement si, elle est le corps des racines sur K pour un polynôme $f(X) \in K[X]$.

Démonstration Si l'extension E de K est finie, alors elle est algébrique et est de la forme $E = K(a_1,...,a_n)$. Soit $P_i(X) = Irr(a_i,K)$ pour $i = 1,2,...,n$ et soit $P(X) = \prod_{i=1}^{i=n} P_i(X)$. Nous allons prouver que E est le corps des racines de P sur K. Tout d'abord, chaque $P_i(X)$ se décompose en produit de facteurs linéaires dans $E[X]$ car il est irréductible, il possède une racine dans E et E est normale sur K. Il en résulte que P se décompose en produit de facteurs linéaires dans $E[X]$ et E est un corps de décomposition pour P sur K. Ensuite, E est un corps de décomposition minimal pour P sur K car si F est un corps de décomposition pour P sur K contenu dans E, alors F doit contenir tous les a_i ce qui prouve $F = E$.

Réciproquement, supposons que E est le corps des racines pour un polynôme $Q \in K[X]$ sur K et soit $f \in K[X]$ un polynôme irréductible ayant une racine a dans E. Soit M le corps des racines de $f.Q$ sur K. M s'écrit $M = K(a_1,...,a_n,b_1,...,b_m)$ où $a_1,...,a_n$ sont les racines de Q dans M et $b_1,...,b_m$ sont celles de f. Nous avons, par le théorème précédent,

$$[E(b_1) : E] = [E(b_i) : E] \text{ pour } i = 2,3,...,m.$$

Si $b_1 \in E$, alors $[E(b_1) : E] = 1 = [E(b_i) : E]$ ce qui prouve $b_i \in E$ pour $i = 2,3,...,m$. Il en résulte $E = M$ et E est un corps de décomposition pour f sur K.

Définition Soit E une extension de K. Une **clôture normale** de E est une extension normale de K qui satisfait les deux conditions suivantes :

1. $K \subseteq E \subseteq N$.
2. Si M est une extension normale de K vérifiant $K \subseteq E \subseteq M \subseteq N$, alors $M = N$.

En d'autre termes, la clôture normale de E est une extension normale minimale de K contenant E.

Exemple $\mathbb{C}$ est une clôture normale de l'extension $\mathbb{R}$ de $\mathbb{Q}$.

Théorème Toute extension finie E de K possède une clôture normale.

Démonstration E, étant une extension finie K, elle est algébrique et elle s'écrit $E = K(a_1,...,a_n)$. Les éléments a_i sont tous algébrique sur K. Soit

$$P_i(X) = Irr(a_i,K) \quad \text{et } P = P_1...P_n.$$

Soit N un corps des racines pour P sur K. N est une extension normale de K contenant E. D'un autre côté, si M est une extension normale de K vérifiant $K \subseteq E \subseteq M \subseteq N$, alors M est un corps de décomposition pour chaque P_i car elle contient une racine pour ce polynôme irréductible. Ainsi, M est un corps de décomposition pour P sur K contenu dans N. Or N est un corps de racines pour P sur K, d'où $M = N$.

Théorème Deux clôtures normales d'une extension finie E de K sont K-isomorphes.

Démonstration D'après ce qui précède, ces deux extensions de K sont deux corps de racines pour le polynôme $P = \prod_{i=1}^{i=n} Irr(a,K)$ sur K. Elles sont K-isomorphes.

Théorème Soit E une extension normale finie de K et F une extension algébrique de K contenant E. Tout K-isomorphisme σ de E dans F est un K-automorphisme de E.

Démonstration E, étant une extension normale finie de K, elle est le corps des racines d'un polynôme $P \in K[X]$ et elle s'écrit $E = K(a_1,...,a_n)$ où $a_1,...,a_n$ sont les racines du polynôme P. Il suffit de prouver $\sigma(E) \subseteq E$, car E est un K-espace vectoriel de dimension finie et σ est un endomorphisme injectif de cet espace vectoriel. Or $\sigma(a_i)$ est une racine de P pour $i = 1,2,..,n$. Il en résulte $\sigma(a_i) \in E$ pour $i = 1,2,..,n$. et par suite $\sigma(E) \subseteq E$.

Théorème Soit E une extension normale finie de K et F un corps intermédiaire entre K et E. Tout K-isomorphisme σ de F dans E peut être prolongé en un K-automorphisme de E.

Démonstration E est le corps des racines d'un polynôme $P \in K[X]$ sur K. Il est aussi le corps des racines pour P sur F et sur $\sigma(F)$. Ainsi, le K-isomorphisme σ de F sur $\sigma(F)$ peut être prolongé en un K-isomorphisme de E dans E. Ce prolongement de σ est, en réalité, un K-automorphisme, car E est un K-espace vectoriel de dimension finie.