Algèbre M1 Cours 4

Extensions normale

19 Octobre 2010

Corps de décomposition : le retour

Définition – Corps de décomposition d'une famille de polynôme. Soient k un corps et $\mathscr{F} = (P_i)_{i \in I}$ une famille d'éléments de $k[X]$. *Un corps de décomposition* de la famille $\mathscr{F}$ est une extension K de k telle que tous les éléments de $\mathscr{F}$ sont scindés dans K et K est engendrée sur k par les racines des éléments de $\mathscr{F}$.

Remarque – Une notion pas vraiment nouvelle. Si $\mathscr{F}$ a un seul élément alors c'est précisément la notion déjà vue.
Si $\mathscr{F} = (P_1, \ldots, P_n)$ est une famille finie alors un corps de décomposition pour $\mathscr{F}$ n'est rien d'autre qu'un corps de décomposition pour le polynôme $P = P_1 \cdots P_n \in k[X]$. Ainsi pour les familles finies, on est ramené à ce qu'on connaît déjà.

Corps de décomposition d'une famille

Proposition – Existence et unicité du corps de décomposition. Soient k un corps et $\mathscr{F} = (P_i)_{i \in I}$ une famille d'éléments de $k[X]$. Il existe un corps de décomposition pour la famille $\mathscr{F}$. Si K et K' sont deux corps de décomposition pour la famille $\mathscr{F}$ alors ils sont k-isomorphes.
Plus généralement, si K est un corps de décomposition et L une extension de K dans laquelle tous les P_i sont scindés alors il existe un k-morphisme de K dans L.

Preuve. *Existence.* Considérons Ω une extension algébriquement close de k. Dans Ω, on pose K l'extension engendrée par les racines de l'ensemble des P_i. Comme Ω est algébriquement clos, les P_i sont scindés dans Ω et donc dans K et par définition K est bien sûr engendrée sur k par les racines des P_i.

Fin de la preuve

Unicité. Considérons L une extension de k dans laquelle tous les P_i sont scindés et $j : L \to \Omega$ une extension algébriquement close. Bien sûr, les P_i sont scindés sur $j(L)$. Il existe un k-morphisme $\sigma : K \to \Omega$. Comme K est engendrée par les racines des P_i et que σ envoie une racine de P_i dans K sur une racine de P_i dans Ω , $\sigma(K)$ est contenue dans $j(L)$. Ainsi, on peut factoriser σ par j.

$$\begin{tikzcd}
K \arrow[rr, dotted] \arrow[rrr, bend left, "\sigma"] & & L \arrow[r, "j"] & \Omega \\
& k \arrow[ul, "j^{-1}\circ\sigma"] \arrow[ur] & &
\end{tikzcd}$$

Si K et K' sont deux corps de décompositions de $\mathscr{F}$ alors il existe un k-morphisme σ de K dans K' et un K' dans K (noté τ), on obtient ainsi un k-endomorphisme de K (c'est $\tau\sigma$) et un de K' (c'est $\sigma\tau$) qui sont donc des automorphismes puisque K et K' sont algébriques sur k. Ainsi τ et σ sont surjectifs.

Extensions normales

Définition – Extension normale. Soit $(K : k)$ une extension algébrique. On dit que K est une *extension normale de k* si pour tout P polynôme irréductible sur k ayant une racine dans K alors P est scindé dans K.

Définition – Extension séparable. Soit $(K : k)$ une extension algébrique. On dit que K est une *extension séparable de k* si pour tout P polynôme irréductible sur k ayant une racine dans K alors P est à racines simples dans K.

Exercice Montrer que k est une extension normale de k.
Si Ω est une clôture algébrique de k, montrer que Ω est une extension normale de k.
Si K est une extension de degré 2 de k, montrer que $(K : k)$ est normale.

Caractérisation

Proposition – Caractérisation des extensions normales. Soit $(K : k)$ une extension algébrique. On désigne par L une extension de K, par Ω une extension algébriquement close de k, par M une k-extension contenant K, par $\widetilde{Om}$ une extension algébrique close contenant K et par σ, σ' des k-morphismes. On a alors les équivalences

(i) $(K : k)$ est normale ;

(ii) K est le corps de décomposition d'une famille $\mathscr{F}$ de $k[X]$;

(iii) Pour toute L et tout $\sigma, \sigma' : K \to L$, on a $\sigma(K) = \sigma'(K)$;

(iv) Pour tout $\sigma, \sigma' : K \to \Omega$, on a $\sigma(K) = \sigma'(K)$;

(v) Pour toute M et tout $\sigma : K \to M$, on a $\sigma(K) = K$;

(vi) Pour toute M et tout $\sigma : K \to M$, on a $\sigma(K) \subset K$;

(vii) Pour tout $\sigma : K \to \widetilde{\Omega}$, on a $\sigma(K) = K$

$(viii)$ Pour tout $\sigma : K \to \widetilde{\Omega}$, on a $\sigma(K) \subset K$

La preuve (1)

Preuve. $(v) \Leftrightarrow (vi)$ et $(vii) \Leftrightarrow (viii)$ résultent du fait que σ définit par restriction un endomorphisme d'une extension algébrique de k qui est donc un automorphisme.
De plus, on a évidemment $(v) \Rightarrow (vii)$ et $(iii) \Rightarrow (iv)$.
$(iv) \Rightarrow (iii)$. Considérons $\sigma, \sigma' : K \to L$ alors σ et σ' sont à valeurs dans $L' = \{x \in L, x \text{ algébrique sur } k\}$. On en déduit que $\sigma, \sigma' : K \to L'$. Par ailleurs, comme L' est algébrique sur k, il existe un k-morphisme $j : L' \to \Omega$. On peut alors définir $j\sigma$ et $j\sigma'$ qui sont des k-morphismes de K dans Ω. On en déduit que $j\sigma(K) = j\sigma'(K)$ et $\sigma(K) = \sigma'(K)$ puisque j est injective.
$(vii) \Rightarrow (v)$. Considérons $\sigma : K \to L$ alors σ est à valeurs dans $M' = \{x \in M, x \text{ algébrique sur } k\}$. On en déduit que $\sigma : K \to M'$. Par ailleurs, comme M' est algébrique sur k, on a $M' \subset \widetilde{\Omega}$. On peut alors considérer σ comme un k-morphisme de K dans $\widetilde{\Omega}$. On en déduit que $\sigma(K) = K$.

La preuve (2)

$(i) \Rightarrow (ii)$. Considérons $\mathscr{F}$ la famille des polynômes irréductibles sur k ayant une racine dans K. Par hypothèse tous les polynômes sont scindés dans K et tout élément de K est racine d'un tel polynôme (son polynôme minimal) puisque K est algébrique. Ainsi K est bien engendré sur k par les racines des éléments de $\mathscr{F}$.
$(ii) \Rightarrow (iii)$. Comme K est engendré par les racines des éléments de $\mathscr{F}$, $\sigma(K)$ est engendré par les racines des éléments de $\mathscr{F}$ dans L. Ainsi $\sigma(K)$ est complètement déterminée.
$(iii) \Rightarrow (v)$. Il suffit de prendre $\sigma' = \mathrm{id}_M$.
$(vii) \Rightarrow (i)$. Considérons $P \in k[X]$ un polynôme irréductible ayant une racine x dans K et $\{x = x_1, \ldots, x_n\}$ l'ensemble de ses racines dans $\widetilde{\Omega}$. La propriété universelle des corps de rupture assure que pour tout i, il existe un k-(iso)morphisme $\tau_i : k(x) \to k(x_i)$ envoyant x sur x_i. Comme $k(x_i) \subset \widetilde{\Omega}$ et que $\widetilde{\Omega}$ est algébriquement clos, chacun des τ_i se prolonge à K en $\sigma_i : K \to \widetilde{\Omega}$. On a alors $\sigma_i(x) = x_i \in K$ et P est scindé dans K.

Extension normale et automorphisme

Application – Normalité et automorphisme. Soit $(K : k)$ une extension algébrique, on a

$$|\mathrm{Aut}_k(K)| = |\mathrm{Hom}_{k-\mathrm{alg.}}(K, K)| \leqslant [K : k]_{\mathrm{s}}.$$

En effet, $(K : k)$ est algébrique, donc tout k-endomorphisme de K est un automorphisme de K. Par ailleurs, si Ω est une extension algébriquement close de k et $j : K \to \Omega$ un morphisme de k-extensions alors les $j\sigma : K \to \Omega$ pour $\sigma \in \mathrm{Aut}_k(K)$ forment une famille d'éléments deux à deux distincts (puisque j est injectif).

Le groupe $\mathrm{Aut}_k(K)$ est noté $\mathrm{Gal}(K/k)$ ou $\mathrm{Gal}_k(K)$.

De plus, si $(K : k)$ est une extension normale, on a

$$|\mathrm{Gal}(K/k)| = [K : k]_{\mathrm{s}}.$$

En effet, considérons $\widetilde{\Omega}$ une extension algébriquement close contenant K. Le critère (*vii*) de normalité assure que $\mathrm{Hom}_{k-\mathrm{alg.}}(K, \widetilde{\Omega}) = \mathrm{Hom}_{k-\mathrm{alg.}}(K, K)$.

Extension normale finie

Remarque – Extension normale finie. Soit $(K : k)$ une extension finie. Alors K est normale sur k si et seulement si K est le corps de décomposition d'un polynôme.
En effet, comme $(K : k)$ est finie, on peut écrire $K = k(x_1, \ldots, x_n)$ et K est le corps de décomposition de $P = P_1 \cdots P_n \in k[X]$ où P_i est le polynôme minimal de x_i sur k. En effet, P est scindé puisque chacun des P_i l'est (puisque $(K : k)$ est normale) et K est bien engendré par les racines de P (puisqu'il l'est déjà par $x_1, \ldots, x_n$ qui sont des racines de P).

Extension galoisienne

Remarque – Extension normale et séparable finie. Soit $(K : k)$ une extension finie. Alors K est normale et séparable sur k si et seulement si K est le corps de décomposition d'un polynôme irréductible séparable.

($\Rightarrow$) En effet, comme $(K : k)$ est finie et séparable, on peut écrire $K = k(x)$ et K est le corps de décomposition de $P \in k[X]$ le polynôme minimal de x sur k. En effet, P est scindé (puisque $(K : k)$ est normale) et K est bien engendré par les racines de P (puisqu'il l'est déjà par x qui sont des racines de P).

($\Leftarrow$) $(K : k)$ est normale puisque K est un corps de décomposition sur k et $(K : k)$ est séparable puisque K est engendré par des éléments séparable sur k (les racines du polynôme irréductible).

Exemples

Exemple – Un exemple classique. L'extension $\mathbb{Q}(j, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2})$ est normale : c'est le corps de décomposition de $X^3 - 2$. Par contre, l'extension $\mathbb{Q}(\sqrt[3]{2})$ ne l'est pas : le polynôme $X^3 - 2$ est irréductible sur $\mathbb{Q}$ mais n'a pas toutes ses racines dans $\mathbb{Q}(\sqrt[3]{2})$.

Une sous-extension d'une extension normale n'est pas nécessairement normale.

Exemple – Normalité et transition. L'extension $(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ est normale puisqu'elle est de degré 2, de même, l'extension $(\mathbb{Q}(\sqrt[4]{2} : \mathbb{Q}(\sqrt{2}))$ est normale. Mais l'extension $(\mathbb{Q}(\sqrt[4]{2} : \mathbb{Q}))$ n'est pas normale puisque le polynôme $X^4 - 2$ irréductible sur $\mathbb{Q}$ n'a pas toutes ses racines dans $\mathbb{Q}(\sqrt[4]{2})$.

La normalité n'est pas une propriété transitive.

Les restes de la transitivité

Remarque Soient $(K : k)$ et $(L : K)$ deux extensions telle que $(L : k)$ est normale. Alors $(L : K)$ est normale.
En effet, si L est le corps de décomposition sur k d'une famille $\mathscr{F}$ alors L est encore le corps de décomposition de $\mathscr{F}$ sur K.

Clôture normale

Définition – Clôture normale. Soit $(K : k)$ une extension. Une *clôture normale* de K est une extension N de K vérifiant les deux propriétés suivantes :

1. $(N : k)$ est normale ;
2. Si N' est une sous-K-extension de N telle que $(N : k)$ soit normale alors $N' = N$.

Proposition – Existence et unicité de la clôture normale. Soit $(K : k)$ une extension. Alors K admet une clôture normale N. De plus, si $\sigma : K \to M$ est un k-morphisme à valeurs dans M une extension **normale** de k. Alors il existe un K-morphisme de N dans M (c'est-à-dire un « prolongement » de σ à N).

$$\begin{tikzcd}
N \arrow[rr, dotted] & & M \\
& K \arrow[ul] \arrow[ur, "\sigma"'] & \\
& k \arrow[u] \arrow[uur] &
\end{tikzcd}$$

En particulier, deux clôtures normales de K sont isomorphes.

Preuve

Preuve. *Existence.* Soit N un corps de décomposition de la famille $\mathscr{F}$ des polynômes irréductibles sur k ayant une racine dans K. Montrons que N est une clôture normale de K sur k.

L'extension $(N : k)$ est normale.

Montrons à présent que N est bien une extension de K. Comme deux corps de décomposition de $\mathscr{F}$ sont k-isomorphes, il suffit de trouver un corps de décomposition M de l'ensemble des polynômes irréductibles sur k qui est une extension de K. On aura alors $j : K \to M$ et par composition avec un k-isomorphisme $\sigma : M \to N$, on obtiendra que N est une extension de K.

On considère alors M le corps de décomposition de $\mathscr{F}$ formé de l'ensemble des racines des éléments de $\mathscr{F}$ dans une extension algébriquement close Ω de k. Comme Ω est algébriquement clos, il existe un k-morphisme τ de K dans Ω. De plus, si $x \in K$ alors le polynôme minimal P est dans $\mathscr{F}$ et donc $\tau(x) \in M$ est une racine de P dans Ω. Ainsi $\tau : K \to M$.

Suite de la preuve

Considérons à présent N' une sous-K-extension N qui est normale sur k. Pour tout $x \in K$, le polynôme minimal de $x \in K$ sur k admet une racine dans N' (puisque N' est une sous-K-extension) donc est scindé dans N' (puisque $(N' : k)$ est normale). Ainsi N' contient toutes les racines des éléments de $\mathscr{F}$ et donc $N \subset N'$ puisque N est engendrée par ces racines.

Montrons à présent qu'une clôture normale N est toujours un corps de décomposition sur K de la famille $\mathscr{F}$. Comme N est une extension de K, tout élément P de $\mathscr{F}$ à une racine dans N (l'image d'une racine de P dans K par le morphisme de K dans N est une racine de P dans N) donc est scindé dans N (puisque N est normale sur k). La sous-k-extension N_1 de N engendrée par les racines des éléments de $\mathscr{F}$ dans N est alors un corps de décomposition de $\mathscr{F}$ dans N. En particulier, c'est une sous-K-extension de N qui est normale sur k et donc $N = N_1$ puisque N est une clôture normale.

Propriété de morphismes

Soit M une extension de K qui est normale sur k. On note $j : K \to \Omega$ une extension algébriquement close. Comme Ω est algébriquement clos, Ω est une K-extension de M et de N. On a

$$\begin{tikzcd}
N \arrow[rr, "\sigma"] & & \Omega \\
& K \arrow[ul] \arrow[ur] & M \arrow[u, "\tau"']
\end{tikzcd}$$

Tout élément de $\mathscr{F}$ admet une racine dans M (puisque c'est une K-extension) et donc est scindé dans M (puisque $(M : k)$ est normale). Ainsi, tout élément de $\mathscr{F}$ est scindé dans M et donc dans $\tau(M)$.

Comme N est un corps de décomposition pour $\mathscr{F}$ sur k, N (resp. $\sigma(N)$) est engendré sur k par les racines des éléments de $\mathscr{F}$ dans N (resp. $\sigma(N)$). Or les racines des éléments de $\mathscr{F}$ sont dans $\tau(M)$. Ainsi $\sigma(N) \subset \tau(M)$ et on peut considérer « $\tau^{-1}\sigma$ ».

Propriété de morphismes

Soit M une extension de K qui est normale sur k. On note $j : K \to \Omega$ une extension algébriquement close. Comme Ω est algébriquement clos, Ω est une K-extension de M et de N. On a

$$\begin{tikzcd}
N \arrow[rr, dotted] \arrow[rrr, bend left, "\sigma"] & & M \arrow[r, "\tau"] & \Omega \\
& K \arrow[ul, "\tau^{-1}\sigma"] \arrow[ur] & &
\end{tikzcd}$$

Tout élément de $\mathscr{F}$ admet une racine dans M (puisque c'est une K-extension) et donc est scindé dans M (puisque $(M : k)$ est normale). Ainsi, tout élément de $\mathscr{F}$ est scindé dans M et donc dans $\tau(M)$.

Comme N est un corps de décomposition pour $\mathscr{F}$ sur k, N (resp. $\sigma(N)$) est engendré sur k par les racines des éléments de $\mathscr{F}$ dans N (resp. $\sigma(N)$). Or les racines des éléments de $\mathscr{F}$ sont dans $\tau(M)$. Ainsi $\sigma(N) \subset \tau(M)$ et on peut considérer « $\tau^{-1}\sigma$ ».

Fin de la preuve : unicité

Si N et N' sont deux clôtures normales de K alors il existe un K-morphisme σ de N dans N' et un de N' dans N (noté τ), on obtient ainsi un K-endomorphisme de N (c'est $\tau\sigma$) et un de N' (c'est $\sigma\tau$) qui sont donc des automorphismes puisque N et N' sont algébriques sur K. Ainsi τ et σ sont surjectifs.

Remarque – Autre preuve. Démontrer la « propriété de morphismes » et « l'unicité » en démontrant qu'une extension normale est un corps de décomposition de $\mathscr{F}$ sur K (et pas seulement sur k).