

Existence et unicité à isomorphisme près du corps de rupture, et degré

Pierre Lissy

April 29, 2010

Lemme 1. *On a existence du corps de rupture.*

Proof. L'anneau $K[X]$ est principal et le polynôme P est irréductible. Donc l'idéal (P) est premier dans $K[X]$, donc maximal car $K[X]$ est principal et par propriété $K[X]/(P)$ est un corps. De plus, K s'injecte dans $L = K[X]/(P)$ car P étant irréductible, il est notamment non inversible donc de degré supérieur ou égal à 1. On peut donc considérer $x \in K \mapsto x + (P)$ qui est injective. De plus, dans L , on a, en posant $x = X + (P)$, si $P(X) = \sum a_i X^i$, alors dans L on a $P(x) = \sum a_i x^i = \sum a_i (X + (P))^i = \sum a_i X^i + (P) = (P)$ qui est l'élément nul dans L . Donc $P(x) = 0$ et L est bien un corps de rupture de K . Enfin, par division euclidienne, ce nouveau corps est de degré $n = \deg(P)$. En effet, si $Q \in K[X]$, alors $Q = BP + R$ avec $\deg(R) < \deg(Q)$. Donc dans L le polynôme réduit Q est égal à R . Ceci montre que $(1, x, \dots, x^{n-1})$ est une famille génératrice du K -espace vectoriel L . cette famille est libre car si $\sum a_i x^i = 0$ dans L , Alors le polynôme $\sum a_i X^i$ dans $K[x]$ est de degré strictement inférieur à $\deg(P)$ mais est tel que P le divise. Donc il est forcément nul, ie $a_i = 0$ pour tout i . On a donc bien ce qu'on voulait. $\square$

Pour l'unicité, considérons plusieurs lemmes.

Lemme 2. *Tout isomorphisme i entre deux corps K et K' se prolonge de manière unique en un isomorphisme de $K[X]$ sur $K'[X]$ envoyant le monôme X sur le monôme X . Ce nouvel isomorphisme sera noté $\bar{i}$.*

Proof. C'est évident. On pose $\bar{i} : \sum a_i X^i \mapsto \sum i(a_i) X^i$. C'est clairement un morphisme d'anneaux (car i en est un), il envoie X sur X , il est surjectif car si $\sum (b_i) X^i \in K'[X]$ alors un antécédent possible est $\sum i^{-1}(b_i) X^i$, et injectif car $\sum i^{-1}(a_i) X^i = 0$ implique que pour tout i , $i(a_i) = 0$ et i étant injectif on a $a_i = 0$ pour tout i . $\square$

Lemme 3. *Soit L et L' deux corps de rupture de deux polynômes P et $P' = \bar{i}(P)$ sur K et K' (qui sont isomorphes par i) engendrés par une racine x et x' . Il existe un unique morphisme de L sur L' prolongeant i et vérifiant $\varphi(x) = x'$.*

Proof. On a un morphisme $U : K[X] \mapsto L$ qui à un polynôme P associe $P(x)$. Il est surjectif par définition du corps de rupture qui est une extension monogène $K[x]$. Son noyau est l'ensemble des éléments tel que $Q(x) = 0$. mais P étant irréductible, c'est le polynôme minimal de P et donc $\text{Ker}(U) = PK[X]$. On a donc par passage au quotient un isomorphisme $u : K[X]/(P) \rightarrow L$. On a de même un isomorphisme $u' : K'[X]/(P') \rightarrow L'$. L'isomorphisme $\bar{i}$ construit à la question précédente induit alors par passage au quotient un isomorphisme entre $K[X]/(P)$ et $K'[X]/(P')$, noté j . En effet, on a un morphisme surjectif de $K[X]$ vers $K'[X]/(P')$ par composition avec la projection canonique, et son noyau est l'ensemble des polynômes $Q = \sum a_i X^i$ tel que $P' = i(P)$ divise $\sum i(a_i) X^i = \bar{i}(Q)$. On a donc $\bar{i}(P)R = \bar{i}(Q)$ et $P\bar{i}^{-1}(R) = Q$. Donc le noyau est $PK[X]$, d'où l'isomorphisme. Finalement, l'isomorphisme $u'ju^{-1}$ convient alors: $u'ju^{-1}(x) = u'j(Cl_K(X)) = u'(Cl_{K'}(X)) = x'$. $\square$

On conclut en prenant $K = K'$.