Unicité du corps de rupture et de décomposition

Maximilien Dreveton

July 8, 2016

Références Perrin p. 70 (notations pas terrible avec P' qui n'est pas la dérivée de P)
Szpirglas p. 727
RWM

0.1 Recasages

Passe à l'aise 123 Corps finis. Applications. (on insiste sur $Dec(X^q - X)$ est le corps à q éléments; et corps de rupture permet de construire explicitement des corps fini à partir de F_p et un polynôme irréductible du bon degré)

125 Extensions de corps. Exemples et applications.

141 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

144 Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications. (F_q est un corps de racine, corps de rupture = adjonction de racines, corps de décomposition permet d'éviter de se placer dans la clôture algébrique)

Arnaques 122 Anneaux principaux. Exemples et applications. (on quotiente par l'idéal d'un polynôme irred : utilise que K[X] principal)

0.2 Le développement

Théorème 0.1. *Il existe un corps de rupture de P sur K, unique à isomorphisme près.*

Proof. Pour l'existence, $L := K[X]/(P)$ convient.

En effet, K s'injecte dans L et pour $x = \pi(X)$ (π projection canonique), on a $P(x) = \pi(P(X)) = 0$.

Comme X engendre $K[X]$ et π surjectif, x engendre L donc $L = K(x) = K[x]$. □

Lemme 0.2. *$i : K \to \tilde{K}$ un isomorphisme de corps, $P \in K[X]$ irréductible, $\tilde{P} = i(P)$. Soit L (resp $\tilde{L}$) un corps de rupture de P sur K (resp de $\tilde{P}$ sur $\tilde{K}$), engendré par une racine x de P (resp x' de $\tilde{P}$).*

Alors

$$\exists! \phi : L \to \tilde{L} \text{ isomorphisme tel que } \phi(x) = x' \text{ et } \phi_K = i$$

Proof. $u : K[X] \to L; X \mapsto x$ morphisme. Im(u) = K[x] = L et Keru=(P).

Donc par passage au quotient $K[X]/(P) \approx L$

De même, on a $\tilde{K}[X]/(\tilde{P}) \approx \tilde{L}$.

Enfin $\tilde{K}[X]/(\tilde{P}) \approx K[X]/(P)$ (par l'isomorphisme $i : K \to \tilde{K}$ qui s'étend en $K[X] \to \tilde{K}[X]$ d'image $(\tilde{P})$ et noyau (P)).

□

Théorème 0.3. *Soit $P \in K[X]$ quelconque.*

Il existe un corps de décomposition, unique à isomorphisme près.

Proof. Pour l'existence, on procède par récurrence sur deg P.

deg P = 1 : L=K convient.

Si P=produit de facteurs de degré 1 (P scindé), alors L=K convient aussi. Sinon, soit Q facteur irréductible de P, $degQ \geq 2$.

Soit K' un corps de rupture de Q sur K, et x racine de Q engendrant K'.

On a : $P(X) = (X - x)R(X)$ dans $K'[X]$. deg R =n-1 donc par HR il existe L corps de décomposition de R sur K'.

Mais en fait, L est corps de décomposition de L sur K. En effet, R admet n-1 racines $x_2, \ldots, x_n$ sur L et $L = K'(x_2, \ldots, x_n) = K(x_1)(x_2, \ldots, x_n) = K(x_1, x_2, \ldots, x_n)$.

□

Lemme 0.4. *Soient K et $\tilde{K}$ deux corps isomorphe, notons i l'isomorphisme.*

Soit $P \in K[X]$, on note $\tilde{P} = i(P)$.

Soient L (resp $\tilde{L}$) corps de décomposition de P (resp i(P)) sur K (resp $\tilde{K}$).

Alors $\exists \phi : L \to \tilde{L}$ isomorphisme prolongeant i.

Proof. (Impérativement voir Szpirglas pour le schéma) Récurrence sur $[L : K]$.

Si L=K on a L'=K'.

Sinon, soit $\alpha \in L - K$ racine de P et Q polynôme minimal de α. Q est un facteur irréductible de P.

$\tilde{Q} = i(Q)$ est facteur irréductible de $\tilde{P}$, et soit α' racine de $\tilde{Q}$ dans $\tilde{L}$.

$M := K[\alpha]$ corps de rupture de Q sur K

$M' := K[\alpha']$ corps de rupture de $\tilde{Q}$ sur $\tilde{K}$. Donc ces deux corps sont isomorphes par le lemme précédent. Notons j l'isomorphisme; il prolonge i.

On a dans M: $P(X) = (X - \alpha)S(X)$, et dans M' : $\tilde{P}(X) = (X - \alpha')S'(X)$ avec j(S)=S'.

Donc L est un corps de décompo de S sur M; L' est corps de décompo de S' sur $\tilde{M}$: par HR il existe ϕ un isomorphisme entre les deux prolongeant j, donc prolongeant i. □

0.3 Compléments

Proposition 0.5. *$P \in K[X]$, deg P$\geq$ 1. L corps de décompo de P sur K. Alors $[L : K]$ divise n!*

Proof. Voir RWM. □

Exemple classique : $P(X) = X^3 - 2 \in \mathbb{Q}[X]$.

Corps de rupture de degré 3, engendré par une des 3 racines. Ils sont différents mais isomorphes.

Corps de décompo de degré 6 (degré 2 sur le corps de rupture).