MATHÉMATIQUES DISCRÈTES (2)

Michel Rigo

http://www.discmath.ulg.ac.be/

Année 2007–2008

Extension par un élément algébrique

Hypothèse de travail

$\mathbb{K}$, $\mathbb{L}$ deux champs, $\mathbb{L}$ extension de $\mathbb{K}$.

Définition

$\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ si $\exists\, P \in \mathbb{K}[X]$ t.q. $P(\alpha) = 0$.

Idéal annulateur

$$\mathcal{P}_\alpha = \{P \in \mathbb{K}[X] \mid P(\alpha) = 0\}$$

$\mathbb{K}[X]$ est principal, il existe un polynôme M_α (monique) t.q.

$$\boxed{\mathcal{P}_\alpha = \{P \in \mathbb{K}[X] \mid P(\alpha) = 0\} = \langle M_\alpha \rangle.}$$

On appelle M_α le polynôme minimum de α.

Si $\alpha' \in \mathbb{L} : M_\alpha(\alpha') = 0$, alors α' est un conjugué de α sur $\mathbb{K}$.

Extension par un élément algébrique

Lemme

Soit $\alpha \in \mathbb{L}$ un élément algébrique sur $\mathbb{K}$ ayant M_α comme polynôme minimum.

I) Le polynôme M_α est irréductible sur $\mathbb{K}$.

II) Pour tout $P \in \mathbb{K}[X]$, $P(\alpha) = 0$ SSI M_α divise P.

III) M_α est l'unique polynôme monique de degré minimum dans $\mathbb{K}[X]$ annulé par α.

IV) Si P est un polynôme monique irréductible sur $\mathbb{K}$ annulé par α, alors $P = M_\alpha$.

Extension par un élément algébrique

i) P.A. Si $M_\alpha = P.Q$ avec $0 < \deg P, \deg Q < \deg M_\alpha$.

Alors, $M_\alpha(\alpha) = P(\alpha).Q(\alpha) = 0$ et P ou $Q \in \mathcal{P}_\alpha$.

Donc, M_α doit diviser P ou Q. Impossible vu les degrés.

ii) Immédiat.

iii) Tout polynôme monique de $\mathbb{K}[X]$ annulé par α appartient à $\mathcal{P}_\alpha$ et est donc un multiple de M_α. Par conséquent, il est soit égal à M_α soit de degré strictement supérieur.

Extension par un élément algébrique

iv) Immédiat, $\mathcal{P}_\alpha = \langle M_\alpha \rangle$

OU...

Soit P polynôme monique irréductible sur $\mathbb{K}$ annulé par α.

Division euclidienne : $P = Q.M_\alpha + R$ avec $\deg R < \deg M_\alpha$.

a) $R = 0$. Puisque P est irréductible, $Q = 1$ et $P = M_\alpha$.

b) $R \neq 0$. Alors $P(\alpha) = R(\alpha) = 0$

vu iii), impossible car $\deg R < \deg M_\alpha$.

Extension par un élément algébrique

Remarque

Si α' est un conjugué de α, alors ils ont le même polynôme minimum, i.e., $M_\alpha = M_{\alpha'}$.

$M_\alpha(\alpha') = 0$ donc $M_\alpha \in \mathcal{P}_{\alpha'} = \langle M_{\alpha'} \rangle$ (i.e., $M_{\alpha'}$ divise M_α).

Or M_α et $M_{\alpha'}$ sont 2 polynômes moniques irréductibles.

Exemple

Le nombre d'or $\tau = (1 + \sqrt{5})/2 \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$ car il est racine du polynôme

$$M_\tau(X) = X^2 - X - 1$$

Son conjugué est $(1 - \sqrt{5})/2$.

Extension par un élément algébrique

Théorème

L'élément $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ SSI $[\mathbb{K}(\alpha) : \mathbb{K}]$ est fini.

En particulier, $[\mathbb{K}(\alpha) : \mathbb{K}]$ = degré du polynôme minimum de α sur $\mathbb{K}$.

La démonstration découle de quelques remarques...

Extension par un élément algébrique

Remarque

Si $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ et si $\deg M_\alpha = d$,
alors tout élément de l'extension de champ $\mathbb{K}(\alpha)$ s'exprime comme combinaison linéaire à coefficients dans $\mathbb{K}$ des éléments

$$1, \alpha, \ldots, \alpha^{d-1}$$

(Autrement dit, comme un polynôme en α à coefficients dans $\mathbb{K}$ et de degré $< d$.)

Partie 1. Elément particulier de $\mathbb{K}(\alpha)$ (en fait $\in \mathbb{K}[\alpha]$)

$$P(\alpha) = \sum_{i=0}^{n} k_i \, \alpha^i, \quad k_i \in \mathbb{K}$$

Extension par un élément algébrique

Division euclidienne : $P(X) = Q(X).M_\alpha(X) + R(X)$, $\deg R < d$.
Evaluer cette expression en α : $P(\alpha) = R(\alpha)$. OK

Partie 2. Elément arbitraire de $\mathbb{K}(\alpha)$

$$P(\alpha).(Q(\alpha))^{-1}, \text{ avec } \deg P, \deg Q < d$$

Puisque $\deg Q < \deg M_\alpha$, $\langle M_\alpha \rangle \subsetneq \langle Q, M_\alpha \rangle$

M_α irréductible, $\langle M_\alpha \rangle$ maximal donc $\langle Q, M_\alpha \rangle = \mathbb{K}[X] \ni 1$.

De là, il existe des polynômes S, T tels que $1 = S.M_\alpha + T.Q$

Evaluant cette expression en α : $(Q(\alpha))^{-1} = T(\alpha)$

$P(\alpha).(Q(\alpha))^{-1}$ se ramène à un produit de 2 polynômes en α, conclusion vu Partie 1.

CONCLUSION

$(1, \alpha, \alpha^2, \ldots, \alpha^{d-1})$: partie génératrice de $\mathbb{K}(\alpha)$.

Linéairement indépendants sur $\mathbb{K}$ car sinon,

relation linéaire à coefficients dans $\mathbb{K}$ les liant
donc polynôme de degré $< d$ de $\mathbb{K}[X]$ annulé par α !

Extension par un élément algébrique

Réciproque...

Remarque

Si $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ fini, alors les $n+1$ éléments

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

sont linéairement dépendants sur $\mathbb{K}$.

$\Rightarrow$ relation linéaire à coefficients dans $\mathbb{K}$ liant ces éléments, i.e., α est algébrique sur $\mathbb{K}$.

Exemple : τ nombre d'or

$$\frac{2\tau^2 + \tau - 3}{\tau^3 + \tau^2 - \tau + 4} = \frac{10}{22}\tau - \frac{7}{22}$$

$\mathbb{Q}(\tau) = \{a\tau + b \mid a, b \in \mathbb{Q}\}$.

Extension par un élément algébrique

Proposition

L'ensemble des éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$ est un sous-champ de $\mathbb{L}$.

Thèse : si α, β alg. sur $\mathbb{K}$, alors $\alpha+\beta$, $\alpha.\beta$, $-\alpha$ et α^{-1} aussi.

Thèse : $\alpha+\beta$, $\alpha.\beta$, $-\alpha$ et α^{-1} appartiennent à une extension de $\mathbb{K}$ de degré fini (cf. thm...).

α alg. sur $\mathbb{K}$ donc $M=\mathbb{K}(\alpha)$ extension de deg. fini de $\mathbb{K}$.

β alg. sur $\mathbb{K}$ donc alg. sur M.

donc $M'=M(\beta)$ extension de degré fini de M et $M'\subset\mathbb{L}$.

"base télescopique", $[M':\mathbb{K}]=[M':M][M:\mathbb{K}]$
donc M' extension de $\mathbb{K}$ de degré fini.

M' champ $\ni\alpha$, β, donc $M'\ni\alpha+\beta$, $\alpha.\beta$, $-\alpha$ et α^{-1}.

Extension par un élément algébrique

construire des champs finis “par extension”...

Proposition

Soient $\mathbb{L}$ extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$ algébrique sur $\mathbb{K}$.
L'anneau quotient $\mathbb{K}[X]/\langle M_\alpha \rangle$ est isomorphe à l'extension de champ $\mathbb{K}(\alpha)$.

Premier théorème d'isomorphie : “$A/\ker\Phi \cong \operatorname{Im}\Phi$”

$$\Phi : \mathbb{K}[X] \to \mathbb{L} : P \mapsto P(\alpha)$$

Φ homomorphisme d'anneaux, $\ker\Phi = \mathcal{P}_\alpha = \langle M_\alpha \rangle$ maximal.

$$\mathbb{K}[X]/\ker\Phi \text{ est un champ} \cong \operatorname{Im}\Phi.$$

pour conclure, a-t-on $\operatorname{Im}\Phi = \{P(\alpha) \mid P \in \mathbb{K}[X]\} = \mathbb{K}(\alpha)$?

Extension par un élément algébrique

$$\Phi : \mathbb{K}[X] \to \mathbb{L} : P \mapsto P(\alpha)$$

$\alpha \in \operatorname{Im}\Phi$ (prendre $P(X) = X$)
$\mathbb{K} \subset \operatorname{Im}\Phi$ (prendre $P(X) = k$, $\forall k \in \mathbb{K}$).

donc $\mathbb{K}(\alpha) \subset \operatorname{Im}\Phi$.

L'autre inclusion :
Soit $P(\alpha)$ un élément quelconque de $\operatorname{Im}\Phi$, $P \in \mathbb{K}[X]$.

$$P(\alpha) = k_0 + k_1\,\alpha + \cdots + k_d\,\alpha^d, \quad k_0, \ldots, k_d \in \mathbb{K}$$

et appartient donc à $\mathbb{K}(\alpha)$!

Extension par un élément algébrique

Application

$P(X) = X^2 + X + 2$ irréductible sur $\mathbb{Z}_3[X]$.

Dans $\mathbb{L} = \mathbb{Z}_3[X]/\langle P \rangle$ (extension de $\mathbb{Z}_3$), $\alpha = X + \langle P \rangle$ annule P.

$$P(\alpha) = X^2 + X + 2 + \langle P \rangle = 0 + \langle P \rangle$$

$\alpha \in \mathbb{L}$ algébrique sur $\mathbb{Z}_3$ avec P comme polynôme minimum.

Ainsi, $\mathbb{Z}_3(\alpha)$ est un champ à 9 éléments

$$0,\ 1,\ 2,\ \alpha,\ \alpha+1,\ \alpha+2,\ 2\alpha,\ 2\alpha+1,\ 2\alpha+2.$$

On y effectue les sommes et les produits comme dans $\mathbb{Z}_3[\alpha]$ en se rappelant que $\alpha^2 + \alpha + 2 = 0$.

Par exemple, on a $(1 + 2\alpha)(2 + 2\alpha) = \alpha^2 + 2 = 2\alpha$.

Extension par un élément algébrique

Suite...

	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
1	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
2	2	1	2α	$2+2\alpha$	$1+2\alpha$	α	$2+\alpha$	$1+\alpha$
α	α	2α	$1+2\alpha$	1	$1+\alpha$	$2+\alpha$	$2+2\alpha$	2
$1+\alpha$	$1+\alpha$	$2+2\alpha$	1	$2+\alpha$	2α	2	α	$1+2\alpha$
$2+\alpha$	$2+\alpha$	$1+2\alpha$	$1+\alpha$	2α	2	$2+2\alpha$	1	α
2α	2α	α	$2+\alpha$	2	$2+2\alpha$	$1+2\alpha$	$1+\alpha$	1
$1+2\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$	α	1	$1+\alpha$	2	2α
$2+2\alpha$	$2+2\alpha$	$1+\alpha$	2	$1+2\alpha$	α	1	2α	$2+\alpha$

Extension par un élément algébrique

Un autre élément

$\beta = 2X + 2 + \langle P \rangle = 2\alpha + 2$ est aussi tel que $P(\beta) = 0$.

$$P(\beta) = (2X+2)^2 + 2X + 2 + 2 + \langle P \rangle = X^2 + X + 2 + \langle P \rangle = 0 + \langle P \rangle.$$

On aurait également pu construire l'extension $\mathbb{Z}_3(\beta)$, isomorphe à $\mathbb{Z}_3(\alpha)$ par l'isomorphisme envoyant α sur β et laissant les éléments de $\mathbb{Z}_3$ inchangés.

Extension par un élément algébrique

Remarque

L'exemple s'adapte à un champ arbitraire $\mathbb{K}$ et à un polynôme irréductible P de $\mathbb{K}[X]$ de degré d.

Si $\mathbb{K}$ est fini et contient t éléments et si α "annule" P, alors $\mathbb{K}(\alpha)$ est un champ à t^d éléments.

Si $\mathbb{K}$ est un champ et si α et β annulent un même polynôme irréductible $P \in \mathbb{K}[X]$, alors $\mathbb{K}(\alpha)$ et $\mathbb{K}(\beta)$ sont isomorphes par l'isomorphisme envoyant α sur β et laissant les éléments de $\mathbb{K}$ inchangés.