Existence et "unicité" d'une clôture algébrique [1]

A) L'énoncé et deux résultats préliminaires

A1. Théorème de Steinitz (1910) *Tout corps (commutatif) K admet une clôture algébrique, unique à K-isomorphisme (non unique) près.*

La preuve utilise le lemme de Zorn, qui repose sur l'axiome du choix :

A2. Lemme de Zorn *Soit $(\mathcal{E}, \leq)$ un ensemble ordonné tel que toute chaîne (sous-ensemble totalement ordonné) de $\mathcal{E}$ possède un majorant (on dit alors que $\mathcal{E}$ est inductif). Alors $\mathcal{E}$ possède un élément maximal.*

On rappelle que ce "lemme" permet d'établir le théorème de Krull, dont nous utiliserons le

A3. Corollaire *Soient A un anneau commutatif et I un idéal de A. Il existe un idéal maximal de A qui contient I.*

La preuve générale du théorème A1 consiste en une vaste généralisation des constructions de corps de rupture et de décomposition. Les énoncés intermédiaires donnés ici sans preuve constituent de *bons exercices* sur le cours (sans recours au lemme de Zorn).

B) Preuve de l'existence

B1. Exercice Soit $\Omega \supset K$ une extension, où le corps Ω est algébriquement clos. Le sous-corps L des éléments de Ω qui sont algébriques sur K est algébriquement clos ; par suite L est une clôture algébrique de K.

Vu cet exercice il nous suffit de construire un corps algébriquement clos contenant K.

L'étape délicate est la suivante :

B2. Prop : *Pour tout corps K il existe une extension de corps $\Omega_1 \supset K$ telle que tout polynôme non constant de $K[X]$ possède une racine dans Ω_1.*

dém : Pour tout polynôme $f \in K[T] \setminus K$, on considère une indéterminée X_f, et on considère l'anneau des polynômes $A = K[(X_f)_{f\in K[T]\setminus K}] = \{P(X_{f_1}, \dots, X_{f_n}) \in K[X_{f_1}, \dots, X_{f_n}] | n \geq 0; f_1, \dots, f_n \in K[T] \setminus K\}$. Autrement dit, c'est la réunion des anneaux de polynômes $K[X_{f_1}, \dots, X_{f_n}]$, lorsque $\{f_1, \dots, f_n\}$ parcourt les parties finies de $K[T] \setminus K$. On considère l'idéal I de A engendré par les éléments $f(X_f)$, $f \in K[T] \setminus K$. Montrons que $I \neq A$. Dans le cas contraire, on aurait $1 \in I$ donc il existerait un entier $n \geq 1$, des polynômes $f_1, \dots, f_n \in K[T] \setminus K$ et des éléments $h_1, \dots, h_n \in A$ tels que $1 = h_1 f_1(X_{f_1}) + \dots + h_n f_n(X_{f_n})$. Remarquons que chaque f_i possède une racine α_i dans D un corps de décomposition du produit $f_1 \dots f_n$ sur K. En appliquant le morphisme de K-algèbres de A dans D qui envoie X_{f_i} sur α_i, pour $1 \leq i \leq n$, (et les autres indéterminées X_f par exemple sur 0), on obtient alors la contradiction $1 = 0$. Ainsi, $I \neq A$, et par A3 il existe un idéal maximal $\mathcal{M}$ de A contenant I. L'anneau quotient $L_1 = A/\mathcal{M}$ est alors un corps. Considérons le morphisme de K-algèbres $\iota : K \to L_1$, et notons encore ι le morphisme induit $K[T] \to L_1[T]$ qui envoie T sur T. Alors pour

1. M1 Algèbre 1, octobre 19

tout $f \in K[T]$ non constant, le polynôme $\iota(f)$ a une racine dans L_1. En effet, on a $\iota(f)(\overline{X_f}) = \overline{f(X_f)} = \overline{0}$, car $f(X_f) \in I \subset \mathcal{M}$.

Par transport de structure à partir de (L_1, ι), on construit une extension de corps $\Omega_1 \supset K$ dans laquelle tout polynôme non constant de $K[X]$ possède une racine.

B3. Fin de la construction d'une extension algébriquement close de K Par récurrence, on déduit de B2 une suite $(\Omega_i)_{i\geq 1}$ d'extensions de K vérifiant : $\Omega_i \subset \Omega_{i+1}$ pour tout $i \geq 1$, et tout polynôme non constant de $\Omega_i[X]$ possède une racine dans Ω_{i+1}. On pose alors $\Omega = \cup_{i\geq 1}\Omega_i$; Ω est muni naturellement d'une structure de corps. On conclut grâce à

B4. Exercice Le corps Ω est algébriquement clos.

C) Preuve de l'"unicité"

Soit Ω un corps algébriquement clos. On va montrer des propriétés de prolongement pour les morphismes de corps à valeurs dans Ω.

C1. Exercice **a)** Soit $L = K(x) \supset K$ une extension algébrique monogène, où K est un sous-corps de Ω. On note $P = \mathrm{Irr}(x, K)$. Alors il existe un morphisme de corps $L \hookrightarrow \Omega$ qui prolonge l'inclusion $K \hookrightarrow \Omega$, et le nombre de ces prolongements est égal au nombre de racines distinctes de P dans son corps de décomposition.

b) Soit $L \supset K$ une extension finie, où K est un sous-corps de Ω. Il existe un morphisme de corps $L \hookrightarrow \Omega$ qui prolonge l'inclusion $K \hookrightarrow \Omega$. (*indication :* écrire $L = K(x_1, \ldots, x_r)$ et utiliser a)).

On en déduit l'énoncé plus général :

C2. Lemme *Soit $L \supset K$ une extension algébrique, où K est un sous-corps de Ω. Il existe un morphisme de corps $L \hookrightarrow \Omega$ qui prolonge l'inclusion $K \hookrightarrow \Omega$.*

dém : On applique le lemme de Zorn à l'ensemble non vide $\mathcal{E}$ des paires (M, f), où M est un sous-corps de L contenant K et $f : M \hookrightarrow \Omega$ un prolongement de l'inclusion $K \hookrightarrow \Omega$ à M. $\mathcal{E}$ est partiellement ordonné par la relation

$$(M, f) \leq (N, g) \quad \text{ssi} \quad M \subset N \quad \text{et} \quad g_{|M} = f\,.$$

Si $(M_i, f_i)_i$ est un sous-ensemble totalement ordonné de $\mathcal{E}$, la réunion $M := \cup_{i\in I} M_i$ est un sous-corps de L et on définit de manière unique $f : M \hookrightarrow \Omega$ par $f_{|M_i} = f_i$. La paire (M, f) est alors dans $\mathcal{E}$ et c'est un majorant de la famille $(M_i, f_i)_i$. Il existe donc dans $\mathcal{E}$ un élément maximal (M_0, f_0). Puisque l'extension $L \supset K$ est algébrique, tout élément x de L est algébrique sur K, donc a fortiori sur M_0. L'exercice C1.b) dit que l'on peut alors étendre f_0 en $M_0(x) \hookrightarrow \Omega$. Par maximalité de (M_0, f_0), cela entraîne $M_0(x) = M_0$, c'est-à-dire $x \in M_0$. On a donc $L = M_0$, ce qui prouve le lemme C2.

C3. Fin de la preuve d'unicité Si les extensions $\Omega \supset K$ et $\Omega' \supset K$ sont des clôtures algébriques, l'inclusion $K \hookrightarrow \Omega'$ se prolonge par le lemme C2 en $f\colon \Omega \hookrightarrow \Omega'$. Comme Ω est algébriquement clos, $f(\Omega)$ l'est aussi (écrivez-le !). Or l'extension $\Omega' \supset f(\Omega)$ est algébrique, car $f(\Omega) \supset K$. Il suit donc $f(\Omega) = \Omega'$, et f est un K-isomorphisme (a priori non unique) de Ω sur Ω'.