UNIVERSITÉ DE NICE SOPHIA ANTIPOLIS **2010/2011**
Faculté des Sciences
Département de Mathématiques
Préparation à l'agrégation
Développement : Théorème de l'élément primitif
Réferences : Gourdon, Algèbre

Théorème. *Soit $\mathbb{K}$ un corps de caractéristique zéro, et soit $\mathbb{L}$ une extension de $\mathbb{K}$ de degré fini. Il existe alors un élément $x \in \mathbb{L}$ (dit primitif) tels que $\mathbb{L} = \mathbb{K}[x]$.*

Preuve.

1. (a) Rappeler la définition de la caractéristique d'un corps et montrer qu'un corps de caractéristique zéro est infinie. Existe-t-il de corps infinie de caractéristique positive ?
   (b) Pour tout $x \in \mathbb{L}$, montrer qu'il existe un unique polynôme unitaire de degré minimal $M_x \in \mathbb{K}[X]$ tel que $M_x(x) = 0$ (appelé polynôme minimal de x). Montrer que M_x est irréductible dans $\mathbb{K}[X]$.
   (c) Montrer que les racines de M_x dans son corps de décomposition sont deux à deux distinctes. (Indice : M_x et M'_x sont premiers entre eux.)
2. Soient $x, y \in \mathbb{L}$. Nous alons montrer qu'il existe $z \in \mathbb{L}$ tel que $\mathbb{K}(x, y) = \mathbb{K}(z)$. Soit $\mathbb{M}$ un surcorps de $\mathbb{L}$ sur lequel $M_x M_y$ soit scindé :

$$M_x(X) = \prod_{i=1}^{p}(X - x_i), M_y(X) = \prod_{j=1}^{q}(X - y_j) \quad (\text{avec } x = x_1, y = y_1.)$$

   (a) Montrer qu'il existe $t \in \mathbb{K}^*$ tel que les nombres $x_i + ty_j$, $i = 1, \ldots, p$, $j = 1, \ldots, q$, soient deux à deux distincts. (Indice : $\mathbb{K}$ est infinie.)
   (b) On pose $z = x + ty$. Montrer que le pgcd de $M_y(X)$ et $M_x(z - tX)$ dans $\mathbb{M}[X]$ est $X - y$. En déduire que le pgcd de $M_y(X)$ et $M_x(z - tX)$ dans $\mathbb{K}(z)[X]$ est $X - y$ et donc $y \in \mathbb{K}(z)$.
   (c) Montrer que $\mathbb{K}(x, y) = \mathbb{K}(z)$.
3. Montrer qu'il existe $x \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}[x]$.

Exemple 1. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Exprimer $\sqrt{2}$ et $\sqrt{3}$ comme polynômes en $\sqrt{2} + \sqrt{3}$ à coefficients rationels.

Exercice 1. Le théorème est vrai pour $\mathbb{K}$ fini. (Indice : $\mathbb{L}^*$ est cyclique)

Exercice 2. Soit $\mathbb{K} = \mathbb{F}_p(T, U)$ et soit $\mathbb{L} = \mathbb{K}[x, y]$ où x et y sont racines de $X^p - T$, $Y^p - U$. Alors il n'existe pas $z \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(z)$