

## 125 – Extensions de corps. Exemples et applications.

2013 – 2014

### Question.

Quels sont les automorphismes de  $\mathbb{C}$  stables sur  $\mathbb{R}$  ?

### Réponse.

L'identité et la conjugaison.

### Question.

Combien y a-t-il d'éléments d'ordre 2 dans  $(\mathbb{Z}/p\mathbb{Z})^\times$  pour  $p$  impair ?

### Réponse.

$(\mathbb{Z}/p\mathbb{Z})^\times$  est cyclique d'ordre pair, il y a donc un seul élément d'ordre 2 :  $-1$ .

### Question.

Soit  $L/k$  une extension finie avec  $L$  de caractéristique 0, on note  $\bar{k}$  la clôture algébrique de  $k$ . Donner les morphismes de corps  $\varphi : L \rightarrow \bar{k}$   $k$ -linéaires.

### Réponse.

Par le théorème de l'élément primitif,  $L$  est engendré par un élément  $\alpha$ , il suffit alors de connaître l'image de  $\alpha$  par  $\varphi$ . Or  $\alpha$  est algébrique donc annulé par un polynôme  $P \in k[X]$ , donc  $P(\varphi(\alpha)) = \varphi(P(\alpha))$  et donc  $\varphi(\alpha)$  est une racine de  $P$ .

Par ailleurs,  $P$  est à racines simples car irréductible donc premier avec sa dérivée. Soit  $\beta \in \bar{k}$  une racine de  $P$ , on définit  $\varphi : k[X] \rightarrow \bar{k}$  l'application

évaluation en  $\beta$ , le noyau de  $\varphi$  est  $(P)$  donc on obtient un morphisme  $\bar{\varphi} : k[X]/(P) \rightarrow \bar{k}$  tel que  $\bar{\varphi}(X) = \beta$ , et on a  $k[X]/(P) \simeq k(\alpha)$ .

### Question.

Soit  $\varphi_1, \dots, \varphi_n$  les morphismes définis précédemment par les racines de  $P$ , les conjugués de  $\alpha$  sont les  $\varphi_1(\alpha), \dots, \varphi_n(\alpha)$ . Soit  $x \in L$ , montrer que  $S_x := \sum_{k=1}^n \varphi_k(x) \in k$ .

### Réponse.

$S_\alpha$  est la somme des racines, donc correspond au coefficient devant  $X^{n-1}$  de  $P$ .

On considère  $\psi_x : L \rightarrow L$  l'application multiplication par  $x$  pour  $x \in L$ .

On commence par considérer  $\psi_\alpha$ . La matrice de cette application dans la base canonique de  $L$  sur  $k$  comme  $k$ -ev est la matrice compagnon de  $P$ . On a alors  $\text{tr}(\psi_\alpha) = S_\alpha$  et les valeurs propres de  $\psi_\alpha$  sont les  $\varphi_i(\alpha)$ .

Soit  $x \in L$ , on écrit  $x = Q(\alpha)$  avec  $Q \in k[X]$ . On a alors  $\psi_x = Q(\psi_\alpha)$ , et donc les valeurs propres de  $\psi_x$  sont les  $Q(\varphi_i(\alpha))$ . La trace de  $\psi_x$  est donc la somme de ses valeurs propres, c'est-à-dire  $\sum_{k=1}^n Q(\varphi_k(\alpha)) = \sum_{k=1}^n \varphi_k(Q(\alpha)) = \sum_{k=1}^n \varphi_k(x) = S_x$ . On a donc  $S_x = \text{tr}(\psi_x) \in k$ .

### Question.

Montrer que  $\prod_{k=1}^n \varphi_k(x) \in k$ .

### Réponse.

$\det(\psi_x) = \prod_{k=1}^n Q(\varphi_k(\alpha)) = \prod_{k=1}^n \varphi_k(x)$  d'où le résultat.

### Question.

Montrer que la famille  $(\varphi_i)_{1 \leq i \leq n}$  est  $\bar{k}$ -linéairement indépendante.

### Réponse.

Soit  $\lambda_1, \dots, \lambda_n \in \bar{k}$  tels que  $\sum_{i=1}^n \lambda_i \varphi_i = 0$ .

Alors  $\sum_{i=1}^n \lambda_i \varphi_i(\alpha^k) = 0 = \sum_{i=1}^n \lambda_i \varphi_i(\alpha)^k$  pour tout  $k$ . Or les  $\varphi_i(\alpha)$  sont distincts donc le système de Vandermonde est inversible, donc  $\lambda_i = 0$  pour tout  $i$ .

### Question.

On définit  $\text{tr}(x) := \text{tr}(\varphi_x)$  pour  $x \in L$ . Montrer que  $(x, y) \mapsto \text{tr}(xy)$  est  $k$ -bilinéaire non dégénérée sur  $L$ .

### Réponse.

La  $k$ -bilinéarité est claire. Soit  $x \in L$  tels que  $\text{tr}(xy) = 0$  pour tout  $y \in L$ .  
On a

$$\text{tr}(xy) = \sum_{i=1}^n \varphi_i(x)\varphi_i(y)$$

donc par la question précédente,  $\varphi_i(y) = 0$  pour tout  $i$ , donc  $y = 0$ .