

Fiche de TD no 4

**Exercice 1** (Prolongement des morphismes). Soit  $\phi : K \rightarrow \Omega$  un morphisme de corps, où  $\Omega$  est algébriquement clos. Soit  $K \subset L$  une extension finie. On va montrer que  $\phi$  se prolonge sur  $L$ .

1. Soit  $L = K[a]$ . Soit  $P(X)$  le polynôme minimal de  $a$ ; Soit  $b$  une racine de  $P^\phi$  dans  $\Omega$ .

Montrer qu'il existe l'unique morphisme  $\tilde{\phi} : K[a] \rightarrow \Omega$ , qui prolonge  $\phi$  et tel que  $\tilde{\phi}(a) = b$ .

Combien y-a-t-il de morphismes  $\tilde{\phi} : K[a] \rightarrow \Omega$  qui prolongent  $\phi$  ?

2. Conclure par récurrence.

**Exercice 2** (Elément primitif). Soit  $K \subset L$  une extension finie. On cherche un élément  $\alpha \in L$  tel que  $L = K[\alpha]$ .

A. Soit  $K$  de caractéristique 0.

Soit  $L = K[a, b]$ . On cherche  $\alpha = a - tb$  avec  $t \in K, t \neq 0$ .

1. Soient  $P$  et  $Q$  les polynômes minimaux de  $a$  et  $b$  respectivement.

Soit  $a_1 = a, a_2, \dots, a_m$  et  $b_1 = b, b_2, \dots, b_n$  les racines de  $P$  et  $Q$  dans la clôture algébrique  $\Omega$  de  $L$ .

Soit  $S(X) = P(tX + \alpha), S(X) \in K[\alpha][X]$ . Quelles sont les racines communes de  $S$  et  $Q$  dans  $\Omega$  ?

2. Montrer qu'on peut choisir  $t$  de façon à ce que  $b$  soit la seule racine commune de  $S$  et  $Q$ .

Quel sera alors le pgcd de  $S$  et  $Q$  ?

En déduire que  $b \in K[\alpha]$ . Conclure.

3. Conclure pour le cas général.

4. Combien y-a-t-il de morphismes  $\phi : L \rightarrow \Omega$  qui sont l'identité sur  $K$  ?

5. Montrer que  $\alpha \in L$  est primitif si et seulement si pour tous morphismes distincts  $\phi : L \rightarrow \Omega$  et  $\rho : L \rightarrow \Omega$  qui sont l'identité sur  $K$  on a  $\phi(\alpha) \neq \rho(\alpha)$ .

B. Soit  $K$  un corps fini. Montrer que  $K$  possède un élément primitif sur  $\mathbb{F}_p$ .

**Exercice 3.** Soient  $a_1, \dots, a_n$  des entiers,  $K = \mathbb{Q}[\sqrt{a_1}, \dots, \sqrt{a_n}]$ .

**Partie A.**

1. Montrer que le degré  $[K : \mathbb{Q}]$  est une puissance de 2 .

2. Soit  $\sigma : K \rightarrow \mathbb{C}$  un morphisme de corps. Montrer que  $\sigma$  est déterminé par les valeurs  $\sigma(\sqrt{a_1}), \dots, \sigma(\sqrt{a_n})$ .

Quelles sont les valeurs possibles de  $\sigma(\sqrt{a_1}), \dots, \sigma(\sqrt{a_n})$  ?

3. En déduire que  $\sigma(K) = K$ , donc  $\sigma$  est un automorphisme de  $K$ .

**Partie B.** Pour  $I \subset \{1, \dots, n\}$  soit  $a_I = \prod_{i \in I} \sqrt{a_i}$ , et  $a_\emptyset = 1$ .

1. Montrer que  $(a_I)_{I \subset \{1, \dots, n\}}$  est une famille génératrice de  $K$  comme espace vectoriel sur  $\mathbb{Q}$ .

2. Montrer que les assertions suivantes sont équivalentes :

(i)  $[K : \mathbb{Q}] = 2^n$ .

(ii)  $(a_I)_{I \subset \{1, \dots, n\}}$  est une  $\mathbb{Q}$ -base (linéaire) de  $K$ .

(iii) Toute fonction  $\phi : \{1, \dots, n\} \rightarrow \{1, -1\}$  induit un automorphisme  $\bar{\phi}$  de  $K$  avec  $\bar{\phi}(\sqrt{a_i}) = \phi(i)\sqrt{a_i}$ .

(iv)  $\sqrt{a_{i+1}}$  n'appartient pas à  $\mathbb{Q}[\sqrt{a_1}, \dots, \sqrt{a_i}]$ , ( $i = 0, 1, \dots, n-1$ ), ( $a_0 = 1$ ).

**Partie C.** Soient  $p_1, \dots, p_n$  des nombres premiers distincts,  $K = \mathbb{Q}[\sqrt{p_1}, \dots, \sqrt{p_n}]$ . On propose de montrer que  $[K : \mathbb{Q}] = 2^n$ .

Soit  $K_i = \mathbb{Q}[\sqrt{p_1}, \dots, \sqrt{p_i}]$ ,  $i = 1, \dots, n$  et  $a_I = \prod_{i \in I} p_i$

On va montrer par récurrence que  $\sqrt{p_{j+1}}$  n'appartient pas à  $K_j$ . Supposons le résultat vrai pour  $i \leq j$ .

Supposons (par absurde) que  $\sqrt{p_{j+1}} \in K_j$ . Vérifier que  $\sqrt{p_{j+1}}$  est une combinaison linéaire, notée  $c$ , des  $(a_I)$ ,  $I \subset \{1, \dots, j\}$ , à coefficients dans  $\mathbb{Q}$ .

En considérant les images  $\sigma(c)$  pour  $\sigma$  parcourant tous les automorphismes de  $K_j$ , montrer que  $c = qa_I$  pour certains  $q \in \mathbb{Q}$  et  $I \subset \{1, \dots, j\}$  et conclure que c'est impossible.

**Partie D .**

1. Soient  $k_1, \dots, k_n$  des entiers non-nuls.

Montrer que  $u = k_1\sqrt{p_1} + \dots + k_n\sqrt{p_n}$  est un élément primitif de  $K$ .

[Indication : vérifier que les images  $\sigma(u)$  pour  $\sigma \in \text{Gal}(K/\mathbb{Q})$  sont toutes distinctes.]

2. Supposons maintenant que les entiers  $a_1, \dots, a_n$  sont positifs et que au moins un parmi eux n'est pas un carré dans  $\mathbb{Z}$ . Soient  $k_1, \dots, k_n$  des entiers positifs.

Montrer que  $k_1\sqrt{a_1} + \dots + k_n\sqrt{a_n}$  est irrationnel (avec  $\sqrt{a_i} > 0$ ).

Exemple :  $\sqrt{2} + \dots + \sqrt{n}$  est irrationnel .

3. Est-ce que  $\sqrt{15} \in \mathbb{Q}[\sqrt{10}, \sqrt{42}]$  ?