ALGÈBRE ET GÉOMÉTRIE

Algèbre — extensions de corps

A. CHAMBERT-LOIR

EXERCICE 1

Soit $E \to F$ une extension de corps et soit P, Q des polynômes de $E[T]$.

1 On suppose que P et Q sont premiers entre eux dans $E[T]$. Démontrer qu'ils sont encore premiers entre eux dans $F[T]$.

2 Plus généralement, démontrer que le pgcd de P et Q dans $E[T]$ est un pgcd dans $F[T]$.

EXERCICE 2

Soit E un corps de caractéristique 0 et soit $P \in E[T]$ un polynôme irréductible.

1 Démontrer que P et P' sont premiers entre eux.

2 Démontrer que les racines de P (dans une extension quelconque de E) sont simples.

EXERCICE 3

Soit K un corps et soit Ω une extension de K. Soit E et F des extensions finies de K qui sont contenues dans Ω ; on note $m = [E : K]$ et $n = [F : K]$. On note aussi EF le corps engendré par E et F dans Ω.

1 Soit A une sous-algèbre unitaire de Ω. On suppose que $\dim_K(A)$ est finie. Démontrer que A est un corps, et donc une extension de K.

2 Démontrer que EF est une extension finie de K et que $[EF : K] \leqslant mn$.

3 On suppose m et n premiers entre eux. Démontrer que $[EF : K] = mn$ et $E \cap F = K$.

4 Soit $P \in K[T]$ un polynôme irréductible de degré m. On suppose que m et n sont premiers entre eux. Démontrer que P est irréductible dans $F[T]$.

EXERCICE 4

Soit E un corps infini, soit Ω une extension algébriquement close de E.

1 Soit α, β des éléments de Ω qui sont algébriques sur E ; on note $P = \prod(T - \alpha_i)$ et $Q = \prod(T - \beta_j)$ leurs polynômes minimaux, où $\alpha = \alpha_1$ et $\beta = \beta_1$. On suppose que les racines de P sont simples.

a) Démontrer qu'il existe $u \in E$ tel que $\alpha + u\beta = \alpha_i + u\beta_j$ entraîne $i = 1$ et $\beta_j = \beta$.

b) Soit $\gamma = \alpha + u\beta$ et $F = E(\gamma)$. Quelles sont les racines communes de $P(\gamma - uT)$ et de Q ? Démontrer que le pgcd de $P(\gamma - uT)$ et Q (dans $F[T]$) est égal à $T - \beta$.

c) Démontrer que $\beta \in F$ et en déduire que $E(\alpha, \beta) = E(\gamma)$.

2 Soit F une extension finie de E qui est engendrée par des éléments dont le polynôme minimal est à racines simples. (Cette condition est automatique si E est de caractéristique 0, voir l'exercice 2.) Démontrer qu'il existe $\alpha \in F$ tel que $F = E(\alpha)$.

EXERCICE 5

On dit qu'un point P est *constructible* (à la règle et au compas) s'il existe une suite $P_0, \dots, P_n$ de points du plan tels que $P_0 = O$, $P_1 = (1, 0)$, $P_n = P$, et tels que pour tout $m \in \{2, \dots, n\}$, il existe $i, j, k, \ell \in \{0, \dots, m-1\}$ tels que le point P_m soit obtenu par l'une des trois constructions suivantes :

(i) C'est le point d'intersection de deux droites non confondues (P_iP_j) et (P_kP_ℓ) ;

(ii) C'est l'un des deux points d'intersection de la droite (P_iP_j) et du cercle de centre P_k et passant par P_ℓ ;

(iii) C'est l'un des deux points d'intersection du cercle de centre P_i passant par P_j et du cercle de centre P_k passant par P_ℓ.

On identifie le plan à l'ensemble des nombres complexes.

1 *a*) Démontrer qu'un nombre complexe est constructible si et seulement si sa partie réelle et sa partie imaginaire sont constructibles.

b) Démontrer que l'ensemble des nombres constructibles est un sous-corps de $\mathbf{C}$.

c) Soit a un nombre constructible et soit $b \in \mathbf{C}$ tel que $b^2 = a$. Démontrer que b est constructible.

2 *a*) Dans les trois constructions précédentes, démontrer que z_m est algébrique sur le corps $\mathbf{Q}(z_i, z_j, z_k, z_\ell)$ et que son degré est $\leqslant 2$.

b) Démontrer qu'un nombre complexe z est constructible si et seulement s'il existe une suite finie $(E_0, \dots, E_n)$ de sous-corps de $\mathbf{C}$ telle que $\mathbf{Q} = E_0 \subset E_1 \cdots \subset E_n$, où $[E_m : E_{m-1}] = 2$ pour tout $m \in \{1, \dots, n\}$ et $z \in E_n$. (*Théorème de Wantzel.*)

c) En déduire que si z est un nombre constructible, alors z est algébrique sur $\mathbf{Q}$ et son degré est une puissance de 2.

d) Calculer $\sin(3\alpha)$ en fonction de $\sin(\alpha)$. Démontrer que $\sin(\pi/9)$ n'est pas constructible (*impossibilité de la trisection de l'angle*).

3 Soit a un nombre complexe constructible et soit P son polynôme minimal. Soit E l'extension de $\mathbf{Q}$ engendrée par les racines de P.

a) Soit b une racine de P. Démontrer que b est constructible.

b) En déduire que $[E : \mathbf{Q}]$ est une puissance de 2.

4 Soit a un nombre complexe algébrique et soit P son polynôme minimal ; on note $a = a_1, \dots, a_n$ ses racines dans $\mathbf{C}$ et $E = \mathbf{Q}(a_1, \dots, a_n)$. On pose $m = [E : \mathbf{Q}]$ et on suppose que m est une puissance de 2 ; le but de cette question est de démontrer que a est constructible. (La preuve classique utilise la théorie de Galois, celle-ci est inspirée d'une démonstration classique du théorème de D'Alembert-Gauss.) On raisonne par récurrence sur n.

Soit $\mathscr{P}$ l'ensemble des paires $\{i, j\}$, où $1 \leqslant i, j \leqslant n$. Pour $p \in \mathscr{P}$ et $c \in \mathbf{Q}$, on pose $z_{p,c} = a_i + a_j + c a_i a_j$; on pose aussi $Q_c = \prod_p (T - z_{p,c})$.

a) À l'aide du théorème sur les polynômes symétriques, démontrer que pour tout $c \in \mathbf{Q}$, on a $Q_c \in \mathbf{Q}[T]$.

b) Soit $c \in \mathbf{Q}$. Démontrer que les degrés des facteurs irréductibles de Q_c sont des puissances de 2, et que l'un d'entre eux est de degré $< d$. En utilisant l'hypothèse de récurrence, en déduire qu'il existe $p \in \mathscr{P}$ tel que $z_{p,c}$ soit constructible.

c) Démontrer qu'il existe $p \in \mathscr{P}$ et $c \neq c'$ dans $\mathbf{Q}$ tels que $z_{p,c}$ et $z_{p,c'}$ soient tous deux constructibles.

d) Si $p = \{i, j\}$, en déduire que $a_i + a_j$ et $a_i a_j$ sont constructibles, puis que a_i et a_j sont constructibles.

e) Démontrer que a est constructible.