Université Pierre & Marie Curie — M1 de Mathématiques
MM002 (Algèbre et théorie de Galois) — Automne 2013

TD n°8.

1 Résultant

Exercice 1. Soit K un corps. Soit $A = a_n x^n + \cdots + a_0$ et $B = b_m x^n + \cdots + b_0$ deux polynômes de $K[X]$. On considère l'application linéaire Φ de $K_{m-1}[X] \times K_{n-1}[X]$ dans $K_{n+m-1}[X]$, définie par $\Phi(P, Q) = PA + QB$.

a) Montrer que Φ est injective si et seulement si $\mathrm{pgcd}(A, B) = 1$.

b) Montrer que

$$\mathrm{Res}(A,B) := \det \Phi = \begin{vmatrix} a_n & a_{n-1} & \cdots & & & \cdots\ a_0 & 0 & \cdots & & 0 \\ 0 & a_n & \cdots & & & \cdots & a_0 & 0 & & 0 \\ \vdots & & \ddots & \ddots & & & & & \ddots & \vdots \\ & & & a_n & \cdots & & & & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & \cdots\ b_0 & 0 & \cdots & & & \cdots & 0 \\ 0 & b_m & \cdots & & \cdots & b_0 & 0 & \cdots & & 0 \\ \vdots & & \ddots & \ddots & & & \ddots & & & \vdots \\ \vdots & & & \ddots & \ddots & & & & \ddots & \vdots \\ 0 & \cdots & & \cdots\ b_m & \cdots & & & \cdots & & b_0 \end{vmatrix}$$

c) Calculer $\mathrm{Res}(x^7 - a, x^5 - b)$.

Exercice 2. Soit $A = a_n \prod_{i=1}^{n}(X - \alpha_i)$ et $B = b_m \prod_{i=1}^{m}(X - \beta_i)$.

a) i) Montrer que $\mathrm{Res}(a, B) = a^m$, $\mathrm{Res}(A, b) = b^n$, $\mathrm{Res}(B, A) = (-1)^{nm}\,\mathrm{Res}(A, B)$.

ii) Montrer que $\mathrm{Res}((X - \alpha)A, B) = B(a)\,\mathrm{Res}(A, B)$.

iii) En déduire que $\mathrm{Res}(A, B) = a_m^n \prod_{i=1}^{m} B(\alpha_i) = a_m^n b_n^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j)$..

b) En déduire que $\mathrm{Disc}(A) = \mathrm{Res}(A, A') = \prod_{i=1}^{n} A'(\alpha_i) = a_m^{2m-2}\prod_{i<j}(\alpha_i - \alpha_j)^2$.

Exercice 3. Soit $A = a_m \prod_{i=1}^{m}(X - \alpha_i)$ et $B = b_n \prod_{i=1}^{n}(X - \beta_i)$.

a) Quelles sont les racines de $r(x) = \mathrm{Res}((A(x - y), B(y))$?

b) Construire des polynômes dont les racines sont les α_i^2, les $B(\alpha_i)$.

c) Construire des polynômes dont les racines sont les $\alpha_i - \beta_j$, les $\alpha_i\beta_j$ et les α_i/β_j (si $B(0) \neq 0$).

Exercice 4. Soient K un corps de caractéristique 0 et α, β deux éléments algébriques sur K. Soit $\alpha_1 = \alpha, \ldots, \alpha_n$ et $\beta_1 = \beta, \ldots, b_m$ les racines des polynômes minimaux A et B de α et β.

a) Montrer qu'il existe $n \in \mathbb{Z}$ tel que les $\alpha_i + n\beta_j$ soient tous distincts.

b) Trouver un polynôme annulateur C, sans facteur carré, de $\gamma = \alpha + n\beta$.

c) Soit $L = K(\gamma)$. Que vaut $\mathrm{pgcd}(A(\gamma - nX), B(X))$ dans $L[X]$?

d) En déduire que $K(\alpha, \beta) = K(\gamma)$.

e) En déduire que toute extension finie de corps de caractéristique 0 admet un élément primitif.

2 Séparabilité

Exercice 5. Soient X et Y deux indéterminées et p un nombre premier. On pose

$$K = \mathbb{F}_p(X^p, Y^p) \quad \text{et} \quad L = \mathbb{F}_p(X, Y).$$

(i) Montrer que L est une extension finie de K de degré p^2.
(ii) Montrer qu'il n'existe pas d'élément $\theta \in L$ tel que $L = K(\theta)$.

Exercice 6. Soient K un corps , $F = X^3 - 3X - 1 \in K[X]$ et α une racine de F dans une clôture algébrique de K. Montrer que $K(\alpha)$ est une extension séparable de K.

Exercice 7. Soient K un corps de caractéristique un nombre premier p et f un polynôme irréductible sur K. Montrer que f n'est pas séparable si et seulement si il existe g dans $K[X]$ tel que $f(X) = g(X^p)$.

Exercice 8. Soient K un corps de caractéristique un nombre premier p et L une extension finie de K de degré non divisible par p. Montrer que L est séparable sur K.

Exercice 9. Soient $K = \mathbb{F}_p(X)$ et $P = t^p - X$. Montrer que P n'est pas séparable.

3 Extensions galoisiennes

Exercice 10. Soit $n \in \mathbb{N}^*$. Soit $\Phi_n = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (X - e^{2i\pi k/n}) \in \mathbb{C}[X]$.

a) Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$. En déduire que $\Phi_n \in \mathbb{Z}[X]$.

b) Soit ζ une racine primitive n^{e}de 1 et p un nombre premier premier à n. Soit f et g les polynômes minimaux unitaire sur $\mathbb{Q}$ de ζ et $\zeta' = \zeta^p$. On suppose $f \neq g$.

   i) Montrer que $fg|\Phi_n$ et $f|g(X^p)$.

   ii) Montrer que l'image de Φ_n dans $\mathbb{F}_p[X]$ a un facteur irréductible ayant multiplicité au moins deux, et en déduire une contradiction.

c) En déduire que Φ_n est un polynôme irréductible.

d) Montrer que $\mathbb{Q}(e^{2i\pi/n})$ est une extension galoisienne de $\mathbb{Q}$ et décrire son groupe de Galois.

e) Soit K une extension finie de $\mathbb{Q}$. Montrer que K ne contient qu'un nombre fini de racines de 1.

Exercice 11. Soit a un entier sans facteur carré, différent de $0, 1$ et -1. Soit p un nombre premier. Soit K un corps de décomposition de $X^p - a$ sur $\mathbb{Q}$. Calculer $[K : \mathbb{Q}]$.
Soit $G = \mathrm{Gal}(K/\mathbb{Q})$. Montrer que G a un sous-groupe distingué H isomorphe à $\mathbb{Z}/p\mathbb{Z}$ tel que G/H soit isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*$.

Exercice 12. Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Montrer que K est une extension galoisienne de $\mathbb{Q}$ et décrire son groupe de Galois.

Exercice 13. Soient f un polynôme irréductible de $\mathbb{Q}[X]$ et K le corps de décomposition de f dans $\mathbb{C}$. On suppose que le groupe de Galois de K sur $\mathbb{Q}$ est abélien. Montrer que pour toute racine α de f, on a $K = \mathbb{Q}(\alpha)$.