Fiche 8
16 avril 2014

Exercice 1 (Le discriminant sous diverses formes).
Dans tout l'exercice le discriminant d'un polynôme P sera noté Δ_P.

I. Le discriminant par le déterminant de Vandermonde

Soient K un corps et $P \in K[X]$ est un polynôme unitaire de degré $n \geq 2$, dont on notera les racines $\{\alpha_1, \ldots, \alpha_n\}$ en prenant en compte leurs multiplicités. On définit la matrice $V = (\alpha_i^{j-1})_{1 \leq i,j \leq n}$

1. Montrer que $\det(V) = \prod_{1 \leq j < i \leq n}(\alpha_i - \alpha_j)$.
2. Montrer que ${}^tVV = (s_{i+j-2})_{1 \leq i,j \leq n}$, où $s_k = \alpha_1^k + \ldots + \alpha_n^k$.
3. En déduire une formule pour Δ_P.
4. Appliquer la méthode quand $n = 2$.

II. Le discriminant par les dérivées

1. Soient K un corps, P un polynôme unitaire et irréductible dans $K[X]$ de degré au moins 2. Montrer que Δ_P est donné par la formule
$$(-1)^{\frac{n(n-1)}{2}} N_{K(\alpha)/K}(P'(\alpha)) \quad ,$$
où α est une racine de P, et P' en est la dérivée. Cette formule est aussi égale au produit
$$(-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} P'(\alpha_i) \quad ,$$
n étant le degré de P et les α_i en décrivant les racines.
2. Soit K un corps. On définit $P = X^n + aX + b \in K[X]$ et admet qu'il est irréductible dans $K[X]$. Déterminer Δ_P.
3. Montrer que le groupe de Galois de $X^5 + 20X + 16 \in \mathbb{Q}[X]$ est A_5.

Exercice 2 (Lemmes techniques).

1. **(Corps)** Soit $P \in \mathbb{Q}[X]$ un polynôme unitaire de la forme $X^n - a_1X^{n-1} + a_2X^{n-2} + \ldots + (-1)^n a_n$ telle que pour tout $1 \leq i \leq n$, $a_i = b_i d^{-1}$ avec $b_i, d \in \mathbb{Z}$. Montrer que $d^n P(d^{-1}X) \in \mathbb{Z}[X]$ est unitaire, et que son corps décomposition sur $\mathbb{Q}$ est le même que celui de P sur $\mathbb{Q}$.
2. **(Groupes)** Montrer qu'un sous-groupe transitif de S_n qui contient un $(n-1)$-cycle et une transposition est S_n.
3. **(Groupes)** Montrer que S_n ($n \in \mathbb{N}^*$) est engendré par $(1, \ldots, n)$ et $(1, 2)$. Si p est un nombre premier, alors S_p est engendré par un p-cycle et une transposition.
4. **(Groupes)** Montrer que tout sous-groupe transitif de A_5 est isomorphe à A_5 ou au groupe diédral D_5 ou au groupe cyclique d'ordre 5.

Exercice 3 (Groupes de Galois : exemples).

1. Soient p un nombre premier, $P \in \mathbb{Q}[X]$ unitaire, irréductible sur $\mathbb{Q}$ et de degrée p. Montrer que si P a exactement deux racines imaginaires, alors son groupe de Galois est isomorphe à S_p. Appliquer le résultat au polynôme $X^5 - 4X + 2$.
2. Montrer en faisant des réductions modulo 2, 3 et 5 que le groupe de Galois sur $\mathbb{Q}$ de
$$X^6 + 22X^5 + 21X^4 + 12X^3 - 37X^2 - 29X - 15$$
est isomorphe à S_6.
3. Donner un exemple de polynôme de degré 5 dont le groupe de Galois est d'ordre 5.

Exercice 4 (Groupes de Galois : une construction générale).
On montrera que tout $n \in \mathbb{N}^*$, il existe un polynôme unitaire, irréductible P de degré n dont le groupe de Galois est isomorphe à S_n.

1. C'est une révision. Montrer que pour tout premier p et pour tout $n \in \mathbb{N}^*$, il existe un polynôme unitaire, irréductible de degré n dans $\mathbb{F}_p[X]$.
On fixe $n \in \mathbb{N}^*$.
2. Soient maintenant $Q \in \mathbb{F}_2[X]$ de irréductible, unitaire de degré n, $R \in \mathbb{F}_3[X]$ irréductible, unitaire de degré $n-1$, et $S \in \mathbb{F}_p[X]$ $(p > n-2)$ irréductible, unitaire de degré 2. Montrer qu'il existe $P \in \mathbb{Z}[X]$ unitaire, qui se réduit à Q, XR et $X(X+1)(X+2)\dots(X+n-3)S$, modulo 2, 3 et p respectivement.
3. Montrer que le groupe de Galois est isomorphe à S_n.

Exercice 5 (Norme et trace).
Soit p un nombre premier.

(a) Montrer que le polynôme $X^3 - p \in \mathbb{Q}[X]$ est irréductible sur $\mathbb{Q}$.

Soit α une racine de $X^3 - p$. On pose $K = \mathbb{Q}(\alpha)$.

(b) Déterminer $[K : \mathbb{Q}]$ et comparer les extensions K et $\mathbb{Q}(\alpha^2)$.

(c) Montrer que K est $\mathbb{Q}$-isomorphe à l'ensemble des matrices de la forme

$$\begin{pmatrix} a & pc & pb \\ b & a & pc \\ c & b & a \end{pmatrix} \quad , \quad (a, b, c) \in \mathbb{Q}^3 \quad .$$

En déduire que l'équation $X^3 + pY^3 + p^2Z^3 - 3pXYZ = 0$ admet $(0, 0, 0)$ pour unique solution dans $\mathbb{Q}^3$.

(d) Quel est le polynôme minimal de α^2 sur $\mathbb{Q}$?

Exercice 6 (Norme et trace).
En utilisant la trace et la norme, montrer que $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$ et que $1 + \sqrt[3]{2}$ n'est pas un carré dans $\mathbb{Q}(\sqrt[3]{2})$.

Exercice 7 (Norme et trace).
On pose $P(X) = X^3 + X + 1$ dans $\mathbb{Q}[X]$.

(a) Montrer que le polynôme P est irréductible sur $\mathbb{Q}$ avec une unique racine réelle.

(b) On fixe une racine $\alpha \in \mathbb{C}$ de P et pose $L = \mathbb{Q}(\alpha)$. Déterminer la trace de α^2. Déterminer son polynôme minimal sur $\mathbb{Q}$.

(c) Pour $z \in L$, calculer $\mathrm{tr}_{L/\mathbb{Q}}(z)$.