Fiche 10
22 avril 2015

Exercice 1 (Le corps des nombres constructibles).
Soit $\mathcal{C}$ le plus petit sous-corps de $\mathbb{C}$ stable par $\sqrt{\ }$. On appelle $\mathcal{C}$ *le corps des nombres constructibles.*

(a) Montrer que $e^{2i\pi/15}$ et $e^{2i\pi/17}$sont constructibles.

(b) Pour un nombre complexe z, montrer l'équivalence des trois conditions suivantes :

1. $z \in \mathcal{C}$;
2. l'ordre du groupe de Galois du polynôme minimal de z sur $\mathbb{Q}$ est une puissance de 2 ;
3. il existe une tour d'extensions quadratiques $\mathbb{Q} = K_0 \subset K_1 \subset ... \subset K_n$ telle que $z \in K_n$.

(c) Montrer que $\sqrt[3]{2}$ n'est pas constructible.

(d) Montrer que $e^{2i\pi/n}$ est constructible si et seulement si $n = 2^r p_1 ... p_s$ où $p_1 < ... < p_s$ sont des nombres premiers de la forme : $p_i = 2^{2^{k_i}} + 1$.

Exercice 2 (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

$$(-1)^{\frac{n(n-1)}{2}} N_{K(\alpha)/K}(P'(\alpha)) \ ,$$

où α est une racine de P, et P' en est la dérivée. Cette formule est aussi égale au produit

$$(-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} P'(\alpha_i) \ ,$$

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 3 (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 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 4 (Groupes de Galois non résolubles : un exemple).
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.

Exercice 5 (Groupes de Galois non résolubles : 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 $Q \in \mathbb{F}_2[X]$ 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 $X(X+1)(X+2)\ldots(X+n-3)S$, modulo 2, 3 et p respectivement.
3. Montrer que le groupe de Galois est isomorphe à S_n.

Exercice 6 (Une règle et un compas, c'est tout ce que je veux !).
Dans le plan $\mathbb{R}^2$ on définit par récurrence : $P_0 = \{0, 1\}$, et si $n \geq 1$, P_n est l'ensemble des points de P_{n-1} et des points obtenus de la manière suivante :

– on trace toutes les droites reliant deux points de P_{n-1}, tous les cercles centrés en un point de P_{n-1} et de rayon une distance entre deux points de P_{n-1} ;
– on prend toutes les intersections obtenues (entre deux droites, deux cercles, un cercle et une droite).

On appelle $\cup_{n\geq 0} P_n \subset \mathbb{R}^2$ l'ensemble des points *constructibles à la règle et au compas.*

(a) Déterminer P_1 et P_2.
(b) On rappelle que l'on peut construire à la règle et au compas la médiatrice de deux points, la perpendiculaire à une droite passant par un point donné, la parallèle à une droite passant par un point donné. En déduire que si z_1, z_2 sont constructibles, alors $z_1 + z_2, z_1 - z_2, z_1 z_2, z_1/z_2$ le sont aussi.
(c) Montrer que les racines carrées d'un nombre constructible le sont aussi.
(d) Montrer qu'un $z \in \mathbb{C}$ est constructible si et seulement si le point correspondant dans $\mathbb{R}^2$ est constructible à la règle et au compas.