

ALGÈBRE – DEVOIR À LA MAISON II

Le devoir est à rendre au plus tard le **lundi 9 décembre 2024**. Vous pouvez le rédiger en **français ou en anglais**. Le devoir est à rendre de l'une des façons suivantes : **directement lors de séance de TD** ou **par mail en un UNIQUE fichier pdf avec votre nom** dans le nom du fichier à l'adresse kevin.destagnol@universite-paris-saclay.fr pour le groupe de TD 1. Vous pouvez également bien sûr me contacter à cette adresse mail en cas de questions ou si vous repérez ce qui vous semble être une erreur d'énoncé.

PROBLÈME 1 — ÉQUATIONS DE MORDELL. Pour $k \in \mathbf{Z}$, on notera $E_k : y^2 = x^3 + k$. Mordell a établi en 1920 que pour tout entier k , l'équation E_k possède un nombre fini de solutions $(x, y) \in \mathbf{Z}^2$. L'objet de ce problème est d'étudier quelques valeurs particulières de k .

- On suppose dans cette question que $k = -5$ et on suppose qu'on dispose d'une solution $(x, y) \in \mathbf{Z}^2$ de E_{-5} .
 - Montrer que l'on peut supposer y pair et $x \equiv 1 \pmod{4}$.
 - En écrivant $y^2 + 4 = x^3 - 1 = (x - 1)(x^2 + x + 1)$, aboutir à une contradiction et en déduire que E_{-5} n'a pas de solution entière. On pourra utiliser librement le fait que -1 est un carré modulo p si, et seulement si, $p \not\equiv 3 \pmod{4}$.
- On suppose dans cette question que $k = -2$. On note $\mathbf{Z}[i\sqrt{2}]$ le sous-anneau de \mathbf{C} engendré par $i\sqrt{2}$.
 - Justifier qu'il existe un polynôme à coefficients entier P tel que $\mathbf{Z}[i\sqrt{2}] \cong \mathbf{Z}[X]/(P)$. Établir que $\mathbf{Z}[i\sqrt{2}]$ est un anneau euclidien pour le stathme donné par $N(z) = z\bar{z}$ pour $z \in \mathbf{Z}[i\sqrt{2}]$.
 - Soit à présent $(x, y) \in \mathbf{Z}^2$ une solution de E_{-2} . Justifier que l'on peut supposer x et y impairs.
 - Montrer que $x + i\sqrt{2}y$ et $x - i\sqrt{2}y$ sont premiers entre eux dans $\mathbf{Z}[i\sqrt{2}]$. On pourra penser à utiliser N .
 - Démontrer que $x + i\sqrt{2}y$ et $x - i\sqrt{2}y$ sont des cubes dans $\mathbf{Z}[i\sqrt{2}]$.
 - Déterminer toutes les solutions de E_{-2} .
 - Pouvait-on appliquer cette méthode pour étudier les solutions de E_{-5} ?

PROBLÈME 2 — UNE AUTRE APPROCHE DU GROUPE DE GALOIS. Soit k un corps. Dans tout le problème, on se donne un polynôme $P \in k[T]$ unitaire, irréductible, séparable, de degré $n \geq 1$.

Soit L un corps de décomposition de P sur k . On note x_1, \dots, x_n les racines de P dans L . Par définition, une *relation algébrique* entre les racines de P est un polynôme $R \in k[X_1, \dots, X_n]$ tel que $R(x_1, \dots, x_n) = 0$. On note I_P l'ensemble de ces relations algébriques entre les racines de P .

- Montrer que I_P est un idéal de $k[X_1, \dots, X_n]$ et montrer l'existence d'un isomorphisme de k -algèbres entre $k[X_1, \dots, X_n]/I_P$ et L . Justifier que la connaissance de I_P détermine le polynôme P (et donc ses racines).

On définit G_P comme l'ensemble des permutations $\sigma \in \mathfrak{S}_n$ telles que ¹

$$\forall R \in I_P, \quad \sigma \cdot R \in I_P.$$

- Montrer en utilisant l'isomorphisme de k -algèbre de la question 1. que tout $\sigma \in G_P$ fournit un automorphisme de L laissant k invariant.
- Établir que G_P est un sous-groupe de \mathfrak{S}_n isomorphe à $\text{Gal}(L/k)$.

On cherche maintenant des générateurs de l'idéal I_P . On pose $k_0 = k$ et $k_i = k(x_1, \dots, x_i)$ pour tout $i \in \{1, \dots, n\}$. On note $\mu_i(T) \in k_{i-1}[T]$ le polynôme minimal de x_i sur k_{i-1} et on pose $d_i = \deg(\mu_i)$.

- Montrer que pour tout $i \in \{1, \dots, n\}$, il existe un unique polynôme $R_i \in k[X_1, \dots, X_i]$ vérifiant les propriétés suivantes :
 - Le polynôme R_i est unitaire de degré d_i en X_i ;
 - Pour tout $1 \leq j \leq i - 1$, on a $\deg_{X_j}(R_i) \leq d_j - 1$;
 - On a $R_i(x_1, \dots, x_{i-1}, T) = \mu_i(T)$.
- Montrer que pour tout $i \in \{1, \dots, n\}$, on a un isomorphisme de k -algèbres entre $k[X_1, \dots, X_i]/(R_1, \dots, R_i)$ et k_i . En déduire que $I_P = (R_1, \dots, R_n)$.
- Calculer les groupe de Galois et les générateurs explicites de la question 4. de l'idéal I_P dans les cas suivants :
 - $k = \mathbf{F}_2$ et $P = X^3 + X + 1$;
 - $k = \mathbf{Q}$ et $P = X^3 - 2$;
 - $k = \mathbf{Q}$ et $P = X^4 - 2X^2 + 2$.

Indication : Pour le cas (i), on pourra établir que si α est racine de P , alors α^2 et $\alpha + \alpha^2$ aussi.

1. On rappelle que $\sigma \cdot R(X_1, \dots, X_n) = R(X_{\sigma(1)}, \dots, X_{\sigma(n)})$.

On cherche maintenant à établir une formule explicite générale pour les polynômes R_i . On pose $G = \text{Gal}(L/k) = \{\sigma_1, \dots, \sigma_N\}$. Pour tout $y \in L$, on définit le vecteur

$$Gy = (\sigma_1(y), \dots, \sigma_N(y)) \in L^N.$$

7. Soient $y_1, \dots, y_r \in L$. Montrer que les conditions suivantes sont équivalentes :

- (a) La famille (y_1, \dots, y_r) est k -libre dans L ;
- (b) La famille (Gy_1, \dots, Gy_r) est L -libre dans L^N .

Indication : Pour l'implication non triviale, on pourra considérer une relation de dépendance minimale et évaluer en $\sigma \in G$ pour tout $\sigma \in G$ pour en déduire que les coefficients de cette relation de dépendance sont en réalité dans k .

Dans la suite, on fixe un entier $i \in \{1, \dots, n\}$.

8. Montrer que R_i est l'unique polynôme de $L[X_1, \dots, X_i]$ qui vérifie 4.(i), 4.(ii) et qui s'annule en $(\sigma(x_1), \dots, \sigma(x_i))$ pour tout $\sigma \in G$. L'extension L/k_i est galoisienne et on note $G_i = \text{Gal}(L/k_i)$ son groupe de Galois, qui est un sous-groupe de G .

9. Montrer que pour $\sigma \in G$ et $1 \leq j \leq i$, l'élément $\sigma(x_j)$ ne dépend que de la classe de σ dans l'ensemble quotient G/G_i .

Pour tout $\sigma \in G$, on définit l'ensemble

$$C_{\sigma,i} = \left\{ \tau(x_i) : \tau \in G, \tau|_{k_{i-1}} = \sigma|_{k_{i-1}} \right\} \setminus \{\sigma(x_i)\}.$$

10. Montrer que $C_{\sigma,i}$ ne dépend que de la classe de σ dans l'ensemble quotient G/G_i et préciser le cardinal de $C_{\sigma,i}$.

11. Montrer la formule d'interpolation suivante

$$R_i = X_i^{d_i} - \sum_{[\sigma] \in G/G_i} \sigma(x_i)^{d_i} \left(\prod_{y_1 \in C_{\sigma,1}} \frac{X_1 - y_1}{\sigma(x_1) - y_1} \right) \dots \left(\prod_{y_i \in C_{\sigma,i}} \frac{X_i - y_i}{\sigma(x_i) - y_i} \right)$$

et comparer avec vos résultats en question 6.

REMARQUE.— Noter que cette définition du groupe de Galois est beaucoup plus proche de la définition originelle de Galois que l'on peut trouver ci-dessous, extrait de son *Mémoire sur les conditions de résolubilité des équations par radicaux*, texte manuscrit de 1830, publié en 1846 au *Journal de mathématiques pures et appliquées* après sa redécouverte par Liouville en 1843, près de dix ans après la mort de Galois.

PROPOSITION I.

THÉOREME. « Soit une équation donnée, dont a, b, c, \dots sont les m racines. Il y aura toujours un groupe de permutations des lettres a, b, c, \dots qui jouira de la propriété suivante :

» 1°. Que toute fonction des racines, invariable [*] par les substitutions de ce groupe, soit rationnellement connue ;

» 2°. Réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par les substitutions. »