2. Extensions algébriques (suite)

Nombres constructibles et problèmes grecs classiques

Un point du plan euclidien $\mathbb{R}^2$ est dit constructible s'il peut être obtenu à l'aide d'une règle et d'un compas en un nombre fini d'étapes à partir de l'origine et du point de coordonnées $(0,1)$. On dit qu'un nombre réel x est constructible si le point $(x,0)$ l'est. On vérifie facilement qu'un point (x,y) est constructible si et seulement si x et y le sont. Il est également facile de vérifier que l'ensemble des nombres constructibles est stable pour les opérations d'addition, de soustraction, de multiplication, de division et d'extraction de racine carrée. En particulier c'est un sous-corps de $\mathbb{R}$ et tous les nombres rationnels sont constructibles.

On admettra le théorème suivant :

Théorème 1 (Wantzel (1837)) *Soit $x \in \mathbb{R}$. Alors x est constructible si et seulement s'il existe une tour finie d'extensions $(L_0, \dots, L_k)$ de $\mathbb{Q}$ vérifiant :*
- $L_0 = \mathbb{Q}$;
- L_{i+1} *est une extension quadratique de* L_i *pour tout* $i < k$;
- $x \in L_k \subseteq \mathbb{R}$.

Exercice 2.1
1. Déduire du théorème de Wantzel que si x est constructible alors il existe $n \geq 0$ tel que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^n$.
2. Soit $a \in \mathbb{R}$. Montrer que a est algébrique (sur $\mathbb{Q}$) si et seulement si $\sqrt{a}$ l'est également.
3. Déduire de la transcendance de π [théorème d'Hermite-Lindemann (1882)], l'impossibilité de la quadrature du cercle (i.e. impossibilité de construire un carré de même aire que le disque unité).
4. Montrer l'impossibilité de la duplication du cube (i.e. impossibilité de construire à la règle et au compas, l'arête d'un cube ayant un volume double au cube unité).
5. Montrer que les angles π et $\pi/2$ sont trisectables (un angle θ est trisectable si l'on peut construire à partir deux demi-droites formant l'angle θ, deux demi-droites formant l'angle $\theta/3$ en utilisant uniquement la règle et le compas.)
6. Soit $\phi \in \mathbb{R}$. Vérifier la formule trigonométrique suivante :
$$\cos(3\phi) = 4\cos^3(\phi) - 3\cos(\phi).$$
7. En déduire que $2\cos(\pi/9)$ est racine de $X^3 - 3X - 1$.
8. Montre que $\cos(\pi/9)$ n'est pas constructible. En déduire que $\pi/3$ n'est pas trisectable (i.e. impossibilité de la trisection de l'angle).

Exercice 2.2 (Un élément algébrique de degré 4 qui n'est pas constructible)
1. Montrer que le polynôme $P(X) = X^4 - X - 1$ est irréductible sur $\mathbb{Q}$ et possède 4 racines distinctes x_1, x_2, x_3, x_4 dans $\mathbb{C}$.
2. Montrer que $u = x_1\,x_2 + x_3\,x_4$ est racine du polynôme $X^3 + 4X - 1$.
(On pourra remarquer que $u = t - 1/t$ où $t = x_1x_2$ et calculer $u^4 + 4u^2 - u$.)
3. En déduire que, pour tout i, x_i n'est pas constructible.
4. Montrer que $[\mathbb{Q}(x_1, x_2) : \mathbb{Q}] = 12$ et que si K est le corps des racines de P sur $\mathbb{Q}$, alors $[K : \mathbb{Q}] = 24$.

Unicité de la clôture algébrique

Exercice 2.3 1. Soit σ un morphisme d'un corps K dans un corps algébriquement clos Ω. Soit $L = K(a)$ une extension monogène de K de degré fini. Montrer que l'on peut prolonger σ en un morphisme de L dans Ω.

2. Soit K un corps fini ou dénombrable. Soient Ω_1 et Ω_2 deux clôtures algébriques de K. Montrer qu'il existe un K-isomorphisme de Ω_1 sur Ω_2. (On pourra construire une suite croissante de K-morphismes d'un sous-corps de Ω_1 vers le corps Ω_2 et considérer l'union de cette suite .)
3. En utilisant le Lemme de Zorn, montrer le résultat ci-dessus sans hypothèse de cardinalité sur K. (On considérera pour cela l'ensemble des K-morphismes de L dans Ω_2 pour L extension de degré fini de K (incluses dans Ω_1)).

Automorphismes

Exercice 2.4

1. Déterminer les automorphismes du corps $\mathbb{Q}$.
2. Déterminer les automorphismes du corps $\mathbb{Q}(\sqrt{2})$.
3. Déterminer les automorphismes continus du corps $\mathbb{R}$.
4. Déterminer le groupe de Galois de $\mathbb{C}$ sur $\mathbb{R}$, $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) := \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$.

Exercice 2.5 Soient K est corps et $K(X)$ le corps des fractions rationnelles à coéfficients dans K. Soit $G := \mathrm{Aut}_K(K(X))$.

1. Vérifier que pour $a \in K$, l'application qui à $F(X) \in K(X)$ associe $F(X + a)$ est un automorphisme de $K(X)$.
2. En déduire que si K est infini alors G est infini.
3. Soit $\mathrm{Fix}(G) := \{F \in K(X) | \sigma(F) = F,\ \forall \sigma \in G\}$ le corps fixe de G. Montrer que si K est infini alors $\mathrm{Fix}(G) = K$.