

Fiche 2
28 janvier 2015

Exercice 1 (Automorphismes de corps).

1. Dans ce point, nous déterminerons les automorphismes du corps \mathbb{R} . On fixe un endomorphisme f du groupe additif $(\mathbb{R}, +)$.
 - Montrer que f est \mathbb{Q} -linéaire.
 - Montrer que chacune des conditions ci-dessous implique les suivantes :
 - (a) f est monotone ;
 - (b) il existe $(a, b) \in \mathbb{R}^2$ avec $a < b$ tel que f est bornée sur $]a, b[$;
 - (c) f est continue en 0 ;
 - (d) f est continue.Montrer que si f a au moins une de ces propriétés, alors f est linéaire, et en déduire qu'elle est une homothétie.
 - Déduire la description des automorphismes de corps de \mathbb{R} .
2. Déterminer les automorphismes continus du corps \mathbb{C} .
3. Montrer que l'identité est le seul automorphisme du corps $\mathbb{F}_p(t^{\frac{1}{p}})$ qui laisse fixe les éléments de $\mathbb{F}_p(t)$, où t est transcendant sur \mathbb{F}_p .

Exercice 2 (Groupes de Galois).

1. Soit $\alpha = \sqrt{2 + \sqrt{2}}$.
 - (a) Déterminer $f(X) \in \mathbb{Q}[X]$ le polynôme minimal de α sur \mathbb{Q} .
 - (b) Montrer que $\text{Aut}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.
 - (c) L'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est-elle galoisienne ?
2. Déterminer, en justifiant votre réponse, lesquelles des extensions suivantes sont galoisiennes :
 - \mathbb{C}/\mathbb{R} , $\mathbb{F}_{q^n}/\mathbb{F}_q$ ($n \in \mathbb{N}^*$, q est une puissance non nulle d'un nombre premier p) ,
 - $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ (j racine troisième de l'unité) ,
 - L/\mathbb{Q} (L est le corps décomposition de $X^3 - 3X + 1$) .
3. Déterminer le groupe d'automorphismes du corps de décomposition de $P(X) = X^3 - 3X + 1$ sur \mathbb{Q} .

Exercice 3 (Fractions rationnelles).

1. Soient K un corps de caractéristique différente de 2, $E = K(t_1, \dots, t_n)$ le corps des fractions rationnelles à coefficients dans K et H le sous-groupe de $\text{Gal}(E/K(s_1, \dots, s_n))$ correspondant au groupe alterné \mathfrak{A}_n (les s_1, \dots, s_n sont les polynômes symétriques élémentaires en t_1, \dots, t_n qui sont des transcendants (variables) indépendants). Montrer que le corps des invariants de H est $K(s_1, \dots, s_n, \Delta)$ où $\Delta = \prod_{1 \leq i < j \leq n} (t_i - t_j)$.
2. Soient k un corps, t un élément transcendant sur k et G le sous-groupe d'automorphismes de $\text{Aut}(k(t)/k)$ engendré par les automorphismes

$$\sigma_1 : t \mapsto t^{-1} \quad \sigma_2 : t \mapsto 1 - t .$$

On rappelle que $k(t)$ est le corps des fractions rationnelles à coefficients dans k .

- (a) Montrer que G est isomorphe au groupe symétrique \mathfrak{S}_3 .
 - (b) On définit $f : t \mapsto \frac{(t^2-t+1)^3}{t^2(t-1)^2}$. En utilisant le polynôme $(X^2 - X + 1)^3 - fX^2(X - 1)^2$, montrer que $k(f) = k(t)^G$. En déduire que l'extension $k(t)/k(f)$ est galoisienne.
3. Soient F un corps, t un élément transcendant sur F et $E = F(t)$. Pour tout $u \in E$, on a une forme réduite $u = \frac{f(t)}{g(t)}$ avec f et g dans $F[t]$ et premiers entre eux. On définit le degré de u comme le maximum de ceux de f et de g . Soient X et Y deux indéterminées.
 - (a) Montrer que $f(X) - Yg(X)$ est irréductible dans $F[X, Y]$. En déduire qu'il en est de même dans $F(Y)[X]$.
 - (b) Déduire du point (a) que t est algébrique sur $F(u)$. Quel est son polynôme minimal ?
 - (c) Conclure que $F(t) = F(u)$ si et seulement si u est de la forme $\frac{at+b}{ct+d}$ avec $ad - bc \neq 0$.
 - (d) Décrire $\text{Aut}(E/F)$.

Exercice 4 (Clôture algébrique réelle).

- (a) Déterminer les extensions algébriques de \mathbb{R} .
- (b) Montrer que l'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ n'est pas finie.
- (c) On pose : $R = \overline{\mathbb{Q}} \cap \mathbb{R}$. Montrer que $\overline{\mathbb{Q}} = R(i)$.

Remarque : le théorème d'Artin-Schreier affirme que si K/k est une extension finie et si K est algébriquement clos, alors k est de caractéristique 0, $[K : k] = 2$ et il existe $i \in K$ tel que $i^2 = -1$ et $K = k(i)$.