THÉORIE DE GALOIS I

Exercice 1 (*Le théorème de Chevalley-Warning*)— Soit K un corps fini de cardinal q et de caractéristique p. Étant donné un polynôme $f \in \mathrm{K}[\mathrm{T}_1, \dots, \mathrm{T}_n]$, on pose $\mathrm{S}(f) = \sum_{\mathbf{x} \in \mathrm{K}^n} f(\mathbf{x})$.

1. Calculer $\mathrm{S}(\mathrm{T}_1^{\nu_1} \dots \mathrm{T}_n^{\nu_n})$ pour tout n-uplet $(\nu_1, \dots, \nu_n) \in \mathbb{N}^n$.

2. Soient $f_1, \dots, f_m$ des polynômes dans $\mathrm{K}[\mathrm{T}_1, \dots, \mathrm{T}_n]$ de degrés respectifs $d_1, \dots, d_m$ et soit V l'ensemble de leurs zéros communs dans K^n.

On pose $f = \prod_{i=1}^{m} (1 - f_i^{q-1})$. Calculer $\mathrm{S}(f)$ en fonction de $\mathrm{Card}(\mathrm{V})$ et en déduire le théorème de Chevalley-Warning : *si* $d_1 + \ldots + d_m < n$, $\mathrm{Card}(\mathrm{V})$ *est divisible par* p.

3. Déduire de ce qui précède que, si $d_1 + \ldots + d_m < n$ et si les polynômes $f_1, \dots, f_m$ sont sans termes constants, alors V contient un point $\mathbf{x}$ de K^n distinct de $\mathbf{0} = (0, \dots, 0)$.

Exercice 2 (*Polynômes cyclotomiques sur les corps finis*) — Soit K un corps fini de cardinal q et de caractéristique p et soit $\overline{\mathrm{K}}$ une clôture algébrique de K.

On rappelle que, pour tout entier naturel $n \geq 1$, $\Phi_n \in \mathbb{Z}[\mathrm{T}]$ désigne le n-ème polynôme cyclotomique. Ses racines dans une clôture algébrique de $\mathbb{Q}$ sont les racines *primitives* n-ème de l'unité.

1. Soient $r \geq 0$ et $n \geq 1$ des entiers naturels. Si n est premier à p, démontrer que l'on a $\Phi_{np^r} = (\Phi_n)^{p^{r-1}(p-1)}$ dans $\mathbb{F}_p[\mathrm{T}]$.

2. Soit α un élément de $\overline{\mathrm{K}}^\times$. Démontrer qu'il existe un plus petit entier naturel $n \geq 1$ tel que $\alpha^n = 1$, vérifier que n est premier à p et établir que le degré de α sur K est égal à l'ordre de q dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

3. Soit $n \geq 2$ un entier premier à p. Démontrer que le polynôme Φ_n est séparable dans $\mathrm{K}[\mathrm{T}]$ puis déduire de la question précédente que tous les facteurs irréductibles de Φ_n dans $\mathrm{K}[\mathrm{T}]$ ont le même degré.

4. Démontrer que le polynôme $\mathrm{T}^4 + 1$ est irréductible dans $\mathbb{Q}[\mathrm{T}]$ mais qu'il est réductible dans $\mathbb{F}_p[\mathrm{T}]$ pour tout nombre premier p. Comment peut-on généraliser cette observation ?

Exercice 3 — Soient K un corps et L/K une extension algébrique séparable (ce qui signifie que tout élément de L est racine d'un polynôme séparable dans $\mathrm{K}[\mathrm{T}]$).

Supposons qu'il existe un entier naturel n tel que tout élément de L soit de degré au plus n sur K ; démontrer que L est alors une extension finie de K de degré au plus n.

Exercice 4 — Soit K le corps engendré sur $\mathbb{Q}$ par les éléments $\sqrt{2}$ et i de $\mathbb{C}$.

1. Montrer que K est de degré 4 sur $\mathbb{Q}$ et en donner un élément primitif dont on précisera le polynôme minimal.

2. Démontrer que l'extension $\mathrm{K}/\mathbb{Q}$ est galoisienne et que le groupe de Galois $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

3. Dresser la liste des sous-corps de K.

Exercice 5 — Soient K un corps, $\overline{\mathrm{K}}$ une clôture algébrique de K et L/K une extension finie galoisienne de K dans $\overline{\mathrm{K}}$.

Étant donnés un élément x de L et un conjugué y de x dans $\overline{\mathrm{K}}$ (c'est-à-dire une racine du polynôme minimal de x dans $\overline{\mathrm{K}}$), démontrer que y appartient à L et qu'il existe un élément σ de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ tel que $\sigma(x) = y$. Combien y a-t-il de tels σ ?

Exercice 6 — Soient K un corps, $\overline{\mathrm{K}}$ une clôture algébrique de K et L/K une extension finie galoisienne de K dans $\overline{\mathrm{K}}$ de groupe G. Soit H un sous-groupe de G et soit $\mathrm{E} = \mathrm{L}^{\mathrm{H}}$ l'extension de K dans L fixée par H.

Démontrer que la clôture galoisienne de E dans $\overline{\mathrm{K}}$ est contenue dans L et déterminer le sous-groupe de G lui correspondant.

Exercice 7 — Soient k un corps, $\mathrm{L} = k(\mathrm{T}_1, \ldots, \mathrm{T}_n)$ le corps des fractions rationnelles en n variables à coefficients dans k et soit K le sous-corps de L engendré sur k par les fonctions symétriques élémentaires $\Sigma_1, \ldots, \Sigma_n$.

1. Démontrer que L est une extension galoisienne finie de K de groupe de Galois $\mathfrak{S}_n$.

2. Lorsque le corps k est de caractéristique 0, vérifier que $\mathrm{T}_1 + 2\mathrm{T}_2 + \ldots + n\mathrm{T}_n$ engendre L sur K.

3. Soit $f \in \mathrm{L}$ et soit $\mathrm{H} \subset \mathfrak{S}_n$ le sous-groupe fixant f.Démontrer que l'extension $\mathrm{L}/\mathrm{K}(f)$ est galoisienne de groupe H.

4. Déduire de ce qui précède que toute fraction rationnelle $g \in \mathrm{L}$ ayant le même stabilisateur que f peut s'exprimer comme une fraction rationnelle en f et en les $\Sigma_1, \ldots, \Sigma_n$. Étudier l'exemple explicite $n = 3$, $f = \mathrm{T}_1\mathrm{T}_2 + \mathrm{T}_3$ et $g = \mathrm{T}_3$.

Exercice 8 (*Lemme de Dedekind*) — Soient G un groupe, k un corps et $g_1, \ldots, g_n$ des homomorphismes distincts de G dans le groupe multiplicatif $k^\times$.

1. Démontrer que $g_1, \ldots, g_n$ sont linéairement indépendants sur k.
(Indication : raisonner par l'absurde en considérant une relation de dépendance linéaire ne faisant intervenir aucun coefficient non nul.)

2. Soit K un corps et $\sigma_1, \ldots, \sigma_n$ des homomorphismes distincts de k dans K. Déduire de ce qui précède que $\sigma_1, \ldots, \sigma_n$ sont linéairement indépendants sur K, puis que k est de degré au moins n sur le sous-corps

$$k_0 = \{a \in k \mid \sigma_1(a) = \ldots = \sigma_n(a)\}.$$

Exercice 9 (*Le théorème de la base normale*) — Soit L/K une extension galoisienne finie de groupe G. Nous allons démontrer qu'il existe un élément α de L tel que les $[\mathrm{L} : \mathrm{K}]$-éléments $\sigma(\alpha)$, $\sigma \in \mathrm{G}$, forment une base de L sur K.

1. Démontrer directement cette assertion lorsque le corps K est fini.

2. Supposons maintenant que le corps K soit infini et soit x un élément primitif de L de polynôme minimal $f \in \mathrm{K}[\mathrm{T}]$. Quel que soit $\sigma \in \mathrm{G}$, on pose

$$\mathrm{R}_\sigma = \frac{f}{(\mathrm{T} - \sigma(x))\, f'(\sigma(x))}.$$

(i) Vérifier que $\sum_{\sigma \in \mathrm{G}} \mathrm{R}_\sigma = 1$ puis en déduire que

$${\mathrm{R}_\sigma}^2 \equiv \mathrm{R}_\sigma \pmod f$$

pour tout $\sigma \in \mathrm{G}$.

(ii) Démontrer que le déterminant D de la matrice $(R_{\tau\sigma}))_{(\tau,\sigma)\in \mathrm{G}^2}$ est un élément de $\mathrm{L}[\mathrm{T}]$ tel que $\mathrm{D}^2 \equiv 1 \pmod f$.

(iii) Déduire de ce qui précède qu'il existe un élément y de K tel que, posant $\alpha = \mathrm{R}_1(y)$, L soit linéairement engendré sur K par les $\sigma(\alpha)$, $\sigma \in \mathrm{G}$.