THÉORIE DE GALOIS III

Exercice 1 (*Extensions cycliques : théorie d'Artin-Schreier*) — Soit K un corps de caractéristique $p > 0$.

1. Soit a un élément de K et soit L un corps de décomposition du polynôme $T^p - T + a$ au-dessus de K. Démontrer que l'application

$$\mathbb{F}_p \times L \to L, \ \ (u,x) \mapsto x+u$$

induit un homomorphisme injectif du groupe de Galois de l'extension L/K dans le groupe additif de $\mathbb{F}_p$. En déduire que le polynôme $T^p - T + a$ est soit irréductible, soit scindé sur K.

2. Soit réciproquement L/K une extension finie galoisienne de groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et soit σ un générateur de $\mathrm{Gal}(L/K)$.

(i) Démontrer qu'il existe un élément x de L tel que $\sum_{n=0}^{p-1} \sigma^n(x) = 1$.

(ii) Soit $\alpha = \sum_{n=0}^{p-1} n\sigma^n(x)$. Vérifier que $\alpha \notin K$ et $a = \alpha^p - \alpha \in K$ puis en déduire que L est un corps de décomposition du polynôme irréductible $T^p - T + a$.

Exercice 2 (*Un théorème de Galois*) — Galois a démontré qu'une équation est résoluble par radicaux si et seulement si toute racine s'exprime K-rationnellement en fonction de deux quelconques d'entre-elles.

1. Vérifier que l'ensemble $\mathfrak{B}_p$ des permutations de $\mathbb{Z}/p\mathbb{Z}$ de la forme $x \mapsto ax+b$, $a,b \in \mathbb{Z}/p\mathbb{Z}$, est un sous-groupe transitif et résoluble de $\mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$ d'ordre $p(p-1)$. Vérifier également qu'un élément $x \mapsto ax+b$ de $\mathfrak{B}_p$ est d'ordre p si et seulement si $a = 1$ et $b \neq 0$.

2. Soit réciproquement G un sous-groupe transitif et résoluble du groupe symétrique $\mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$. On considère une suite de composition

$$(1) = G_0 \lhd G_1 \lhd \ldots \lhd G_r = G$$

de G à quotients cycliques d'ordre premier.

(i) Démontrer que chacun des groupes $G_1, \ldots, G_r$ opère transitivement sur $\mathbb{Z}/p\mathbb{Z}$; en déduire que G_1 est engendré par une permutation circulaire τ.

(ii) Vérifier qu'il existe une permutation $\sigma \in \mathfrak{S}(\mathbb{Z}/p\mathbb{Z})$ telle que $\sigma G_2 \sigma^{-1} \subset \mathfrak{G}_p$.

(iii) En raisonnant par récurrence sur r, démontrer que G_1 est un sous-groupe distingué de G et en déduire que $\sigma G \sigma^{-1}$ est un sous-groupe de $\mathfrak{B}_p$.

Soit K un corps, soit $P \in K[T]$ un polynôme irréductible de degré premier p et soit L un corps de décomposition de P ; on identifie le groupe de Galois de l'extension L/K à un sous-groupe du groupe des permutations de l'ensemble des racines de P dans L.

3. Supposons qu'il existe deux racines distinctes $\alpha,\ \beta$ de P dans L telles que $L = K(\alpha,\beta)$.

(i) Vérifier que $[L : K] \leq p(p-1)$.

(ii) Vérifier que le groupe $\mathrm{Gal}(L/K)$ contient une permutation circulaire d'ordre p puis que deux telles permutations engendrent le même sous-groupe.

(iii) Démontrer que le groupe $\mathrm{Gal}(L/K)$ est résoluble.

4. Supposons réciproquement que le groupe $\mathrm{Gal}(L/K)$ soit résoluble. Démontrer que l'on a $L = K(\alpha,\beta)$ pour toutes racines distinctes $\alpha,\ \beta$ de P dans L.

Exercice 3 (*Spécialisation du groupe de Galois*) — I. Soient K un corps, $f \in K[T]$ un polynôme et K' un corps de décomposition de f au-dessus de K ; on note $\mathscr{R}$ l'ensemble des racines de f dans K' et on identifie le groupe $\mathrm{Gal}(K'/K)$ à un sous-groupe du groupe symétrique $\mathfrak{S}(\mathscr{R})$.

On introduit des indéterminées Y_ξ, $\xi \in \mathscr{R}$, et on pose

$$L_\sigma = \sum_{\xi \in \mathscr{R}} \xi Y_{\sigma^{-1}(\xi)}$$

pour toute permutation $\sigma \in \mathfrak{S}(\mathscr{R})$.

1. Vérifier que les polynômes

$$\Pi_f = \prod_{\sigma \in \mathfrak{S}(\mathscr{R})} (Y - L_\sigma) \ \text{ et } \ \Theta_f = \prod_{\sigma \in \mathrm{Gal}(K'/K)} (Y - L_\sigma)$$

appartiennent tous deux à l'anneau $\mathrm{K}[\mathrm{Y},(\mathrm{Y}_\xi)_{\xi\in\mathscr{R}}]$ et que Θ_f est un facteur irréductible de Π_f. Quels sont tous les facteurs irréductibles de Π_f dans $\mathrm{K}[\mathrm{Y},(\mathrm{Y}_\xi)_{\xi\in\mathscr{R}}]$?

2. Vérifier que l'action naturelle du groupe $\mathfrak{S}(\mathscr{R})$ sur $\mathrm{K}[\mathrm{Y},(\mathrm{Y}_\xi)_{\xi\in\mathscr{R}}]$ définie par $\tau(\mathrm{Y})=\mathrm{Y}$ et $\tau(\mathrm{L}_\sigma)=\mathrm{L}_{\tau\sigma}$ permute les différents facteurs irréductibles de Π_f et démontrer qu'une permutation $\sigma\in\mathfrak{S}(\mathscr{R})$ appartient au sous-groupe $\mathrm{Gal}(\mathrm{K}'/\mathrm{K})$ si et seulement si $\sigma(\Theta_f)=\Theta_f$.

II. Supposons que K soit le corps $\mathbb{Q}$ des nombres rationnels et que le polynôme f soit *unitaire* et à coefficients entiers.

1. Vérifier que les polynômes Π_f et Θ_f sont à coefficients entiers.

2. Soit p un nombre premier ne divisant pas $\mathrm{pgcd}(\mathrm{P},\mathrm{P}')\in\mathbb{Z}$. On désigne par $\mathscr{R}_p$ l'ensemble des racines du polynôme séparable $\overline{f}=f\pmod p\in\mathbb{F}_p[\mathrm{T}]$ dans une clôture algébrique de $\mathbb{F}_p$.

(i) Démontrer que, pour toute bijection $\varphi:\mathscr{R}\to\mathscr{R}_p$, la réduction modulo p du polynôme $\Pi_f(\mathrm{Y},(\mathrm{Y}_{\varphi(\xi)}))$ est polynôme $\Pi_{\overline{f}}$. Vérifier également que tout élément de $\mathfrak{S}(\mathscr{R}_p)$ permute les réductions des facteurs irréductibles de Π_f.

(ii) Une bijection $\varphi:\mathscr{R}\to\mathscr{R}_p$ sera dite *admissible* si l'homomorphisme de groupes $\mathfrak{S}(\mathscr{R}_p)\to\mathfrak{S}(\mathscr{R}),\ \sigma\mapsto\varphi^{-1}\sigma\varphi$ envoie le groupe de Galois de l'extension $\mathbb{F}_p(\mathscr{R}_p)/\mathbb{F}_p$ sur un sous-groupe de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$.
Démontrer qu'il existe des bijections admissibles de $\mathscr{R}$ sur $\mathscr{R}_p$ et que deux quelconques d'entre-elles envoient le sous-groupe $\mathrm{Gal}(\mathbb{F}_p(\mathscr{R}_p)/\mathbb{F}_p)$ de $\mathfrak{S}(\mathscr{R}_p)$ sur des sous-groupes conjugués de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$.

III. 1. Soit $f\in\mathbb{Z}[\mathrm{T}]$ un polynôme unitaire de degré n. On suppose qu'il existe trois nombres premiers $p_1,\ p_2$ et p_3 tels que

– le polynôme $f\pmod{p_1}$ soit irréductible ;
– le polynôme $f\pmod{p_2}$ soit le produit d'un facteur irréductible de degré 2 et d'un ou de deux facteur(s) irréductible(s) de degré impair dans $\mathbb{F}_{p_2}[\mathrm{T}]$;
– le polynôme $f\pmod{p_3}$ soit le produit d'un facteur linéaire et d'un facteur irréductible dans $\mathbb{F}_{p_3}[\mathrm{T}]$.

Démontrer que le groupe de Galois G d'un corps de décomposition de f au-dessus de $\mathbb{Q}$ est un sous-groupe transitif de $\mathfrak{S}_n$ contenant une transposition et un cycle de longueurs $n-1$; en déduire que $\mathrm{G}=\mathfrak{S}_n$.

2. Déterminer les groupes de Galois des polynômes $\mathrm{T}^5-\mathrm{T}-1$ et $\mathrm{T}^7-\mathrm{T}-1$.

Exercice 4 (*L'ubiquité des groupes symétriques comme groupes de Galois sur* $\mathbb{Q}$) — Soit $n\geq 1$ un entier naturel. Étant donné un entier naturel $\mathrm{N}\geq 1$, on note $\sigma_n(\mathrm{N})$ le nombre des polynômes unitaires $f\in\mathbb{Z}[\mathrm{T}]$ de degré n dont les coefficients sont majorés par N en valeur absolue et dont le groupe de Galois est $\mathfrak{S}_n$.

Suivant B.L. van der Waerden (*Die Seltenheit der Gleichungen mit Affekt*, Mathematische Annalen **139** (1933)), cet exercice a pour objet d'établir que la proportion $(2\mathrm{N}+1)^{-n}\sigma_n(\mathrm{N})$ de ces polynômes tend vers 1 lorsque N tend vers $+\infty$.

1. Étant donné un nombre premier $p\geq 3$, dénombrer les polynômes unitaires de degré n dans $\mathbb{F}_p[\mathrm{T}]$ qui sont soit irréductibles (*type 1*), soit le produit d'un facteur irréductible de degré 2 et d'un ou de deux facteur(s) irréductible(s) de degré impair (*type 2*), soit le produit d'un facteur linéaire et d'un facteur irréductible (*type 3*) ; vérifier qu'il y en a au moins $p^n/k(n)$, où $k(n)=\max(8(n-2),2n)$.

2. On ordonne les nombres premiers $(p_i)_{i\geq 1}$ par ordre croissant et on note $r(\mathrm{N})$ le plus grand entier r tel que $\mathrm{P}=p_1\dots p_r\leq\mathrm{N}$. Quel que soit $i\in\{1,2\}$, vérifier qu'il y a au plus

$$\left(1-\frac{1}{k(n)}\right)^r\mathrm{P}^n$$

polynômes unitaires et de degré n dans $\mathbb{Z}/\mathrm{P}\mathbb{Z}[\mathrm{T}]$ dont la réduction modulo chacun des nombres premiers $p_1,\dots,p_r$ ne soit pas de type i.

3. Déduire de ce qui précède que l'on a

$$\frac{\sigma_n(\mathrm{N})}{(2N+1)^n}\geq 1-3\left(1-\frac{1}{k(n)}\right)^{r(\mathrm{N})}\quad\text{et donc}\quad\lim_{\mathrm{N}}\frac{\sigma_n(\mathrm{N})}{(2\mathrm{N}+1)^n}=1.$$