TD n°8.

Exercice 1. Soit k un corps et $n > 2$ un entier. On note k_n le corps de décomposition du polynôme $X^n - 1$ sur k.

a) Montrer que l'extension k_n/k est Galoisienne.

b) Notons $\mu_n := \{x \in k_n,\ x^n = 1\}$.

i) Quel est le cardinal de μ_n ? Dans la suite on supposera $(n, \mathrm{car}(k)) = 1$.

ii) Montrer que l'action de $\mathrm{Gal}(k_n/k)$ sur k stabilise μ_n, que l'action induite est fidèle, et qu'elle se fait par automorphismes du groupe μ_n.

iii) En déduire un morphisme $\chi_{n,k} : \mathrm{Gal}(k_n/k) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$, uniquement déterminé par la condition que $\forall \zeta \in \mu_n$, $\sigma(\zeta) = \zeta^{\chi_{n,k}(\sigma)}$.

c) Supposons $k = \mathbb{R}$. Montrer que $k_n = \mathbb{C}$ et $\chi_{n,\mathbb{R}}$ envoie la conjugaison complexe sur $-1 \in (\mathbb{Z}/n\mathbb{Z})^\times$.

d) Supposons $k = \mathbb{F}_p$. Montrer que $k_n = \mathbb{F}_{p^r}$ où r est l'ordre de $\bar{p}$ dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$. Puis montrer que $\chi_{n,\mathbb{F}_p}(\mathrm{Frob}) = \bar{p}$.

e) Soit $k = \mathbb{Q}$. Montrer que $\chi_{n,\mathbb{Q}}$ est un isomorphisme.

Exercice 2. Soit k un corps et $n > 1$ un entier premier à la caractéristique de k. On suppose que k contient une racine primitive n-ème de l'unité.

a) Soit K une extension de k engendrée par un élément α tel que $\alpha^n \in k$.

i) Montrer que K est Galoisienne, et que l'application $\sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$ définit une morphisme de groupes injectif $\mathrm{Gal}(K/k) \hookrightarrow \mu_n$. En déduire que $\mathrm{Gal}(K/k)$ est cyclique.

ii) Montrer que $[K : k]$ est égal à l'ordre de α^n dans le groupe $k^\times/(k^\times)^n$.

b) Soit maintenant K une extension Galoisienne de groupe de Galois cyclique d'ordre n. Notons σ un générateur de $\mathrm{Gal}(K/k)$.

i) Pour $\alpha \in K$ un générateur de l'extension K/k, montrer que la matrice $(\sigma^i(\alpha^j))_{0 \leqslant i,j < n}$ est inversible. En déduire que la famille $1, \sigma, \cdots, \sigma^{n-1}$ est libre dans $\mathrm{End}_{k-\mathrm{ev}}(K)$.

ii) Soit ζ une racine n-ème primitive de 1 dans K. Montrer qu'il existe $x \in K$ tel que

$$\alpha := x + \zeta^{-1}\sigma(x) + \cdots, \zeta^{-(n-1)}\sigma^{n-1}(x) \neq 0.$$

iii) Montrer que $\sigma(\alpha) = \zeta.\alpha$. En déduire que $\alpha^n \in k$ et que α engendre K.

Exercice 3 (Polynômes symétriques)**.** On fixe un entier $n > 1$, on note $A = \mathbb{Z}[X_1, \cdots, X_n]$ et $\mathfrak{S}_n$ le groupe des permutations de l'ensemble $\{1, \cdots, n\}$.

a) Pour $\sigma \in \mathfrak{S}_n$, justifier l'existence d'un unique automorphisme d'anneaux $\tilde{\sigma}$ de A tel que $\tilde{\sigma}(X_i) = X_{\sigma(i)}$ pour tout $i = 1, \cdots, n$. Puis montrer que cela définit une action de $\mathfrak{S}_n$ sur A par automorphismes d'anneaux, et que celle-ci se prolonge en une action sur $K = \mathbb{Q}(X_1, \cdots, X_n)$ par automorphismes de corps.

b) Considérons le polynôme $f = (T - X_1) \cdots (T - X_n) \in A[T]$ et développons-le sous la forme $f = T^n - \Sigma_1 T^{n-1} + \cdots + (-1)^n \Sigma_n$ avec $\Sigma_i \in A$. Montrer que les Σ_i sont invariants par $\mathfrak{S}_n$ et en donner une formule explicite comme polynômes en les X_i.

c) Notons $K^{\mathfrak{S}_n}$ le sous-corps des invariants de K sous $\mathfrak{S}_n$ et $k := \mathbb{Q}(\Sigma_1, \cdots, \Sigma_n)$ le sous-corps de K engendré par les Σ_i. On a donc $k \subset K^{\mathfrak{S}_n}$.

i) Rappeler pourquoi $[K : K^{\mathfrak{S}_n}] \geqslant n!$.

ii) Montrer que K est un corps de décomposition de f sur k et en déduire que $[K : k] \leqslant n!$.

iii) Conclure que $k = K^{\mathfrak{S}_n}$ et que les Σ_i sont algébriquement indépendants sur $\mathbb{Q}$.

d) Notons $A^{\mathfrak{S}_n}$ le sous-anneau des invariants de A sous $\mathfrak{S}_n$ et $B := \mathbb{Z}[\Sigma_1, \cdots, \Sigma_n]$ le sous-anneau de A engendré par les Σ_i.

i) Montrer que tout élément de A est entier sur B (cf TD6).

ii) Montrer que tout élément de k qui est entier sur B est dans B, puis en déduire que $B = A^{\mathfrak{S}_n}$.

On a donc montré le théorème suivant : les Σ_i sont algébriquement indépendants sur $\mathbb{Z}$ et on a $\mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n} = \mathbb{Z}[\Sigma_1, \cdots, \Sigma_n]$

Exercice 4. Soit $f \in \mathbb{Z}[X]$ un polynôme unitaire irréductible. On note K_f un corps de décomposition de f, $G_f := \mathrm{Gal}(K_f/\mathbb{Q})$ son groupe de Galois, $\alpha_1, \cdots, \alpha_n$ ses racines dans K_f, et enfin $A_f := \mathbb{Z}[\alpha_1, \cdots, \alpha_n]$ le sous-anneau de K_f engendré par les α_i.

a) Montrer que l'anneau A_f est stable sous G_f, et libre de rang $[K_f : \mathbb{Q}]$ en tant que groupe abélien.

Soit p un nombre premier et $\bar{f} \in \mathbb{F}_p[X]$ la réduction de f modulo p. On suppose que $\bar{f}$ est séparable, et on fixe un idéal maximal $\mathfrak{m}$ de A_f contenant p.

b) Montrer que le corps $k_{\bar{f}} := A_f/\mathfrak{m}$ est un corps de décomposition de $\bar{f}$ sur $\mathbb{F}_p$ et que la projection $A_f \twoheadrightarrow k_{\bar{f}}$ induit une bijection $\alpha_i \mapsto \bar{\alpha}_i$ entre racines de f dans K_f et racines de $\bar{f}$ dans $K_{\bar{f}}$.

c) Soit $\sigma \in G_f$ tel que $\sigma(\mathfrak{m}) \subset \mathfrak{m}$. Montrer que σ induit, par passage au quotient, un automorphisme $\bar{\sigma}$ du corps $k_{\bar{f}}$.

d) Montrer que $G_{f,\mathfrak{m}} := \{\sigma \in G_f, \sigma(\mathfrak{m}) \subset \mathfrak{m}\}$ est un sous-groupe de G_f et que l'application $\sigma \mapsto \bar{\sigma}$ définit un morphisme de groupes $\rho : G_{f,\mathfrak{m}} \longrightarrow G_{\bar{f}} := \mathrm{Gal}(k_{\bar{f}}/\mathbb{F}_p)$.

e) Montrer que ρ est injectif.

f) Soit $\mathcal{M}$ l'ensemble des idéaux maximaux de la forme $\sigma(\mathfrak{m})$ pour un $\sigma \in G_f$. Montrer que $|\mathcal{M}| = |G_f||G_{f,\mathfrak{m}}|^{-1}$.

g) Montrer que le morphisme produit $A_f \longrightarrow \prod_{\mathfrak{n} \in \mathcal{M}} A_f/\mathfrak{n}$ est surjectif. En déduire que $|G_{f,\mathfrak{m}}| \geqslant [k_{\bar{f}} : \mathbb{F}_p]$, puis que ρ est un isomorphisme.

On a donc montré que, sous l'hypothèse que $\bar{f}$ est séparable, $G_{\bar{f}}$ peut s'identifier à un sous-groupe de G_f (non canoniquement).

h) Soit $\bar{f} = \bar{f}_1 \cdots \bar{f}_r$ la décomposition de $\bar{f}$ en produit de facteurs irréductibles dans $\mathbb{F}_p[X]$, et soit $n_i := \deg(f_i)$. Montrer que la permutation décrivant l'action de Frobenius sur $\{\bar{\alpha}_1, \cdots \bar{\alpha}_n\}$ est un produit $c_1 c_2 \cdots c_r$ de cycles à supports disjoints de longueurs respectives $n_1, \cdots, n_r$.

i) Montrer que les assertions suivantes sont équivalentes :

  i) $\bar{f}$ admet une racine dans $\mathbb{F}_{p^m}$

  ii) $(f, X^{p^m} - X) \neq (1)$ dans $\mathbb{F}_p[X]$.

  iii) $\bar{f}$ posséde un facteur irréductible de degré divisant m.

j) Application. Soit $f = X^5 - X - 1$.

  i) En regardant modulo 3, montrer que $\bar{f}$ est irréductible et en déduire que f aussi.

  ii) Montrer que f se factorise en $f = f_1 f_2 f_3$ dans $\mathbb{R}[X]$, avec $\deg(f_2) = \deg(f_3) = 2$. En déduire que G_f contient un produit de deux transpositions (agissant sur les racines). Peut-on en conclure que $G_f = \mathfrak{S}_5$?

  iii) En regardant modulo 2, montrer que $\bar{f} = \bar{f}_1 \bar{f}_2$ avec f_i irréductible de degré $n_1 = 2$ et $n_2 = 3$. En déduire que G_f contient le produit d'une tranposition et d'un 3-cycle disjoints.

  iv) Montrer que $G_f = \mathfrak{S}_5$.