

FEUILLE DE TD N° 10

Exercice 1 groupe de Galois d'un polynôme sur \mathbb{F}_p

Soit $Q(X)$ un polynôme séparable sur \mathbb{F}_p de degré n . On note $Q = Q_1 \dots Q_l$ sa factorisation en irréductibles sur \mathbb{F}_p .

- Justifier que les Q_i sont deux à deux premiers entre eux.
- Pour tout $1 \leq i \leq l$, on note d_i le degré de Q_i . Montrer que l'image du groupe de Galois $\text{Gal}_{\mathbb{F}_p}(Q)$ dans le groupe de permutations des racines est engendré par une permutation de la forme :

$$\sigma = c_1 \dots c_l$$

où les c_i sont des cycles à supports disjoints de longueurs d_i .

Indication. Considérer le morphisme de Frobenius $x \mapsto x^p$ et pour tout i une racine x_i de Q_i .

Exercice 2 permutations qui préservent un facteur irréductible

Soit $P(X) \in K[X]$ un polynôme séparable de degré n sur un corps K . On note x_1, \dots, x_n ses racines dans un corps de décomposition L de P sur K .

On pose :

$$\theta = x_1 U_1 + \dots + x_n U_n \in L[U_1, \dots, U_n]$$

et :

$$F(U, T) = \prod_{s \in \mathfrak{S}_n} (T - {}^s \theta) \in L[U, T] .$$

- Montrer que $F \in K[U, T]$.
- Soit $F = F_1 \dots F_N$ la décomposition de F en facteurs irréductibles *unitaires* dans $K[U, T]$. Montrer que les F_i sont deux à deux distincts et que l'action de \mathfrak{S}_n , par permutations des variables U_1, \dots, U_n , sur $K[U_1, \dots, U_n, T]$ permute les facteurs irréductibles F_1, \dots, F_N .
- On suppose que $F_1(\theta) = 0$ dans $L[U]$. On note

$$\mathfrak{g} = \{s \in \mathfrak{S}_n : {}^s F_1 = F_1\} .$$

Montrer que l'image de $\text{Gal}_K(P)$ dans \mathfrak{S}_n est dans \mathfrak{g} .

Indication. Si $\sigma \in \text{Gal}_K(P)$, noter $s_\sigma \in \mathfrak{S}_n$ la permutation telle que $\forall 1 \leq i \leq n, \sigma(x_i) = x_{s_\sigma(i)}$ puis vérifier que ${}^{s_\sigma} F_1(\theta) = \sigma^{-1}(F_1(\theta))$.

- Montrer que $\forall \sigma \in \text{Gal}_K(P), F_1(\sigma(\theta)) = 0$. En déduire que

$$\prod_{\sigma \in \text{Gal}_K(P)} (T - \sigma(\theta)) \mid F_1 \text{ dans } L[U, T]$$

puis que

$$\prod_{\sigma \in \text{Gal}_K(P)} (T - \sigma(\theta)) = F_1$$

(car les deux sont dans $K[U, T]$).

- Montrer que si $s \in \mathfrak{g}$, alors F_1 s'annule en ${}^s \theta$. En déduire que l'image de $\text{Gal}_K(P)$ dans \mathfrak{S}_n est \mathfrak{g} .

Exercice 3 calcul du groupe de Galois par réduction mod p

Soit $P(X) = X^n + a_1X^{n-1} + \dots + a_n \in \mathbb{Z}[X]$. Soit p un nombre premier. On suppose P et $P \bmod p$ séparables sur \mathbb{Q} et \mathbb{F}_p . On notera x_1, \dots, x_n les racines de P dans \mathbb{C} et z_1, \dots, z_n celles de $P \bmod p$ dans $\overline{\mathbb{F}_p}$. On note $P \bmod p = \overline{P_1} \dots \overline{P_l}$ la factorisation de $P \bmod p$ dans $\mathbb{F}_p[X]$.

- a) On pose $\theta = x_1U_1 + \dots + x_nU_n \in \mathbb{C}[U_1, \dots, U_n]$. On introduit un nouveau polynôme

$$F(U, T) = \prod_{s \in \mathfrak{S}_n} (T - {}^s\theta) \in \mathbb{C}[U_1, \dots, U_n, T].$$

Montrer que $F(U, T) \in \mathbb{Z}[U_1, \dots, U_n, T]$ et que

$$F \bmod p = \prod_{s \in \mathfrak{S}_n} (T - {}^s\bar{\theta}) \in \mathbb{F}_p[U_1, \dots, U_n, T].$$

Indication. On considérera le polynôme

$$S(U, Y, T) = \prod_{s \in \mathfrak{S}_n} (T - Y_1U_{s(1)} - \dots - Y_nU_{s(n)})$$

qui est symétrique en les Y_i !

- b) Soit $F = F_1 \dots F_N$ la factorisation de $F(U, T)$ en irréductibles unitaires dans l'anneau $\mathbb{Q}[U_1, \dots, U_n, T]$. Vérifier que les F_i sont deux à deux distincts et sont dans $\mathbb{Z}[U, T]$.

On notera G l'image de $\text{Gal}_{\mathbb{Q}}(P)$ dans \mathfrak{S}_n et \overline{G} celle de $\text{Gal}_{\mathbb{F}_p}(P \bmod p)$ dans \mathfrak{S}_n (associées aux numérotations des racines : x_1, \dots, x_n et z_1, \dots, z_n).

- c) Notons $\overline{F}_i = F_i \bmod p$. On suppose que $\overline{F}_1(\bar{\theta}) = 0$. Soit \overline{H} le facteur irréductible de $F \bmod p$ qui annule $\bar{\theta}$. Montrer que \overline{H} divise $F_1 \bmod p$ dans $\mathbb{F}_p[U, T]$. En déduire que $\overline{G} \leq G \leq \mathfrak{S}_n$. *Indication.* D'après l'exercice précédent, $G = \{s \in \mathfrak{S}_n : {}^sF_1 = F_1\}$ et $\overline{G} = \{s \in \mathfrak{S}_n : {}^s\overline{H} = \overline{H}\}$.
- d) Dans le cas général, montrer qu'il existe $s_0 \in \mathfrak{S}_n$ tel que ${}^{s_0}\overline{F}_1(\bar{\theta}) = 0$.
- e) Montrer que $\overline{G} \leq s_0 G s_0^{-1}$.
- f) En déduire que dans l'image de $\text{Gal}_{\mathbb{Q}}(P)$ dans \mathfrak{S}_n il existe une permutation $\sigma = c_1 \dots c_l$ où les c_i sont des cycles à supports disjoints de longueurs : $\deg \overline{P}_1, \dots, \deg \overline{P}_l$.
- g) *Application.* Montrer que sur \mathbb{Q} , $X^5 - X - 1$ est de groupe de Galois \mathfrak{S}_5 et $X^5 + 20X + 16$ de groupe de Galois \mathfrak{A}_5 .

Indications. Pour le premier, réduire mod 2 et mod 5, pour le second, calculer le discriminant et réduire mod 3 et mod 7[†].

†. On pourra vérifier que dans le groupe \mathfrak{A}_5 , il n'y a pas de sous-groupe d'indice 2 ou 4