Feuille de TD n° 12

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 $Q = Q_1...Q_l$ sa factorisation en irréductibles sur $\mathbb{F}_p$.

a) Justifier que les Q_i sont deux à deux premiers entre eux.

b) Pour tout $1 \leq i \leq l$, on note d_i le degré de Q_i. Montrer que l'image du groupe de Galois $\mathrm{Gal}_{\mathbb{F}_p}(Q)$ dans le groupe de permutations des racines est engendré par une permutation de la forme :

$$\sigma = c_1...c_l$$

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 $x_1, ..., x_n$ ses racines dans un corps de décomposition L de P sur K.

On pose :

$$\theta = x_1U_1 + ... + x_nU_n \in L[U_1, ..., U_n]$$

et :

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

a) Montrer que $F \in K[U,T]$.

b) Soit $F = F_1...F_N$ 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 $U_1, ..., U_n$, sur $K[U_1, ..., U_n, T]$ permute les facteurs irréductibles $F_1, ..., F_N$.

c) On suppose que $F_1(\theta) = 0$ dans $L[U]$. On note

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

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

Indication. Si $\sigma \in \mathrm{Gal}_K(P)$, 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 remarquer que $(F_1(\theta))^{s_\sigma} = {F_1}^{s_\sigma}(\theta^{s_\sigma})$.

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

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

puis que

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

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

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

Exercice 3 calcul du groupe de Galois par réduction mod p

Soit $P(X) = X^n + a_1 X^{n-1} + ... + a_n \in \mathbb{Z}[X]$. Soit p un nombre premier. On suppose P et $P \bmod p$ séparables sur $\mathbb{Q}$ et $\mathbb{F}_p$. On notera $x_1, ..., x_n$ les racines de P dans $\mathbb{C}$ et $z_1, ..., z_n$ celles de $P \bmod p$ dans $\overline{\mathbb{F}_p}$. On note $P \bmod p = \overline{P_1}...\overline{P_l}$ la factorisation de $P \bmod p$ dans $\mathbb{F}_p[X]$.

a) On pose

$$\theta = x_1U_1 + ... + x_nU_n \in \mathbb{C}[U_1, ..., U_n],\ \overline{\theta} = z_1U_1 + ... + z_nU_n \in \overline{\mathbb{F}_p}[U_1, ..., U_n]\ .$$

On introduit un nouveau polynôme

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

où $\theta^s = x_1U_{s(1)} + ... + x_nU_{s(n)}$.
Montrer que $F(U,T) \in \mathbb{Z}[U_1, ..., U_n, T]$ et que

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

Indication. On considérera le polynôme

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

qui est symétrique en les Y_i !

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

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

c) Notons $\overline{F_i} = F_i \bmod p$. On suppose que $\overline{F_1}(\overline{\theta}) = 0$. Soit $\overline{H}$ le facteur irréductible de $F \bmod p$ qui annule $\overline{\theta}$. 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, $G = \{s \in \mathfrak{S}_n\ :\ {F_1}^s = F_1\}$ et $\overline{G} = \{s \in \mathfrak{S}_n\ :\ adhH^s = \overline{H}\}$.*

d) Dans le cas général, montrer qu'il existe $s_0 \in \mathfrak{S}_n$ tel que ${}^{s_0}\overline{F_1}(\overline{\theta}) = 0$.

e) Montrer que $\overline{G} \leq s_0 G s_0^{-1}$.

f) En déduire que dans l'image de $\mathrm{Gal}_{\mathbb{Q}}(P)$ dans $\mathfrak{S}_n$ il existe une permutation $\sigma = c_1...c_l$ où les c_i sont des cycles à supports disjoints de longueurs : $\deg \overline{P_1}, ..., \deg \overline{P_l}$.

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 $\bmod 2$ *et* $\bmod 5$*, pour le second, calculer le discriminant et réduire* $\bmod 3$ *et* $\bmod 7$ †.

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