École polytechnique 2022-2023
Théorie de Galois

Feuille d'exercices 10

Exercice 1. Soit $f = X^{10} - 1 \in \mathbb{Z}[X]$. Calculer le groupe de Galois de $(f \mod p) \in \mathbb{F}_p[X]$ selon le nombre premier $p \neq 2, 5$.

Exercice 2. Soient $P = X^5 - 4X + 2 \in \mathbb{Q}[X]$ et $G = \mathrm{Gal}(P, \mathbb{Q})$.

(i). Vérifier que P est irréductible sur $\mathbb{Q}$.

(ii). Montrer que G, vu comme groupe de permutations des racines de P dans $\mathbb{C}$, contient une transposition.

(*Indication : on pourra montrer que P a exactement trois racines réelles ou bien utiliser la factorisation de P modulo 257 en le produit* $(X+91)(X-53)(X-31)(X^2-7X-118)$.)

(iii). Montrer que $G = \mathfrak{S}_5$.

Exercice 3. Montrer que le polynôme $X^5 - X - 1 \in \mathbf{Q}[X]$ n'est pas résoluble par radicaux (on pourra réduire modulo 2 et 3).

Exercice 4. Soit p un nombre premier impair.
(i) Montrer que le discriminant de $X^p - 1$ est

$$(-1)^{\frac{p-1}{2}} p^p.$$

(ii) En déduire que

$$\mathbb{Q}\left[\sqrt{(-1)^{\frac{p-1}{2}} p}\right] \subset \mathbb{Q}[\exp(\frac{2i\pi}{p})].$$

(iii) En déduire que toute extension quadratique de $\mathbb{Q}$ se plonge dans une extension cyclotomique [Il s'agit d'un cas particulier du théorème de Kronecker-Weber, d'après lequel toute extension galoisienne à groupe de Galois abélien se plonge dans une extension cyclotomique].

Exercice 5.

Soit $n \geq 1$, Φ_n le n-ème polynôme cyclotomique, et $K = \mathbb{Q}[\zeta_n]$. Soit p un nombre premier ne divisant pas n.
(i) Montrer que la réduction de Φ_n dans $\mathbb{F}_p[X]$ est à racines simples.
(ii) Montrer qu'il existe un élément $Frob_p$ bien déterminé dans le groupe de Galois de $K/\mathbb{Q}$.
(iii) Déterminer l'élément $Frob_p$ avec l'isomorphisme $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.
(iv) Soit a un entier premier à n. Montrer qu'il existe une infinité de nombre premiers p avec $p = a \pmod n$.

Exercice 6.

(i). Montrer que le polynôme $1 + X + X^2 + X^3 + X^4 \in \mathbb{F}_2[X]$ est irréductible.

(ii). Montrer qu'un 4-cycle et un 3-cycle engendrent $\mathfrak{S}_4$.

(iii). Déterminer le groupe de Galois sur $\mathbb{Q}$ du polynôme $X^4 + X^3 - X^2 + X - 1$.

Exercice 7.

(i). Soit $d \geq 2$ un entier et $p \geq d-2$ un nombre premier différent de 2 et 3. Montrer qu'il existe un polynôme $f \in \mathbb{Z}[X]$ unitaire de degré d tel que :

- la réduction modulo 2 de f soit irréductible dans $\mathbb{F}_2[X]$;
- la réduction modulo 3 de f soit de la forme $XQ(X)$ où $Q(X) \in \mathbb{F}_3[X]$ est irréductible ;
- la réduction modulo p de f ait un facteur irréductible de degré 2 et $d-2$ racines distinctes dans $\mathbb{F}_p$.

(ii). Montrer que le groupe de Galois sur $\mathbb{Q}$ d'un tel polynôme f est isomorphe au groupe symétrique S_d.

Exercice 8. (Stickelberger, 1897) Soient $p \neq 2$ un nombre premier et $f \in \mathbb{F}_p[T]$ unitaire de degré d, supposé de discriminant $\Delta \neq 0$. Montrer que le nombre de facteurs irréductibles de f dans $\mathbb{F}_p[T]$ est congru à d modulo 2 si et seulement si Δ est un carré dans $\mathbb{F}_p^\times$.