Théorie de Galois. Mat 3661

Devoir 4. Date limite: le 20 mars 2019

Pour obtenir le maximum de points, faites **5** problèmes parmi 1-8.

1. (a) Soient m et n entiers positifs qui sont premiers relatifs. Soit ξ_m, ξ_n des racines primitives de l'unité (d'ordre m et n). Montrez que $\xi_m \xi_n$ est une racine primitive de l'unité d'ordre mn.

   (b) Soit ξ_n une racine primitive de l'unité d'ordre n et soit d diviseur de n. Montrez que ξ_n^d une racine primitive de l'unité d'ordre n/d.

2. Démontrez que si n est impair, $\Phi_{2n}(x) = \Phi_n(-x)$.

3. Utilisez la formule d'inversion de Möbius pour montrer que

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

4. Soit ℓ premier. On va trouver la factorisation de $\Phi_\ell(x)$ modulo p. Soit ξ une racine de l'unité d'ordre ℓ.

   (a) Montrez que si $p = \ell$, alors $\Phi_\ell(x) = (x-1)^{\ell-1}$ dans $\mathbb{F}_\ell[x]$.

   (b) Supposons que $p \neq \ell$ et soit f l'ordre de p modulo ℓ, alors, f est le plus petit entier positif tel que $p^f \equiv 1 \pmod{\ell}$. Montrez que le polynôme minimal de ξ sur $\mathbb{F}_p$ a degré f.

   (c) Montrez que $\mathbb{F}_p(\xi) = \mathbb{F}_p(\xi^a)$ pour n'importe quel entier a tel que $\ell \nmid a$. Montrez que $\Phi_\ell(x)$ est le produit de $(\ell-1)/f$ polynômes irréductibles de degré f.

5. Soit $K/\mathbb{Q}$ le corps de décomposition de $p(x) = x^6 - 32$. Décrivez les éléments de $\mathrm{Aut}(K/\mathbb{Q})$. À quel groupe abstract est-il isomophe?

6. Montrez que l'extension $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ est cyclique d'ordre 4. (Galoisienne, avec groupe de Galois cyclique.)

7. Soit $p > 2$ premier positif. Soit K est le corps de décomposition de $x^p - 2$. Montrez que $\mathrm{Gal}(K/\mathbb{Q})$ est isomorphe au groupe S de matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \quad a, b \in \mathbb{F}_p,\ a \neq 0.$$

8. Montrez que si le groupe de Galois du corps de décomposition d'un polynôme cubique sur $\mathbb{Q}$ est cyclique d'ordre 3 toutes les racines du polynôme sont réelles.

Problèmes sugérés (à ne pas remettre) du Dummit et Foote :
13.6.10, 13.6.14-17, 14.1.1, 14.1.4,