Université Paris 7-Denis Diderot — Algèbre – Année 2007-08

M1 mathématiques

DEVOIR à rendre le 21 décembre 2007

Soit p un nombre premier impair. Notons $\mu_p = \{e^{2ik\pi/p} / 0 < k \leq p-1\}$ l'ensemble des racines primitives p-ème de 1 dans $\mathbf{C}$ et $\mu_p^+ = \{e^{2ik\pi/p} / 0 < k \leq (p-1)/2\}$. On rappelle que le p-ème polynôme cyclotomique $\Phi_p \in \mathbf{Z}[X]$ est donné par $\Phi_p(X) = (X^p - 1)/(X-1) = \prod_{\zeta\in\mu_p}(X - \zeta)$ et est irréductible sur $\mathbf{Q}$. On pose $\Phi_p^+(X) = \prod_{\zeta\in\mu_p^+}(X - \zeta - \zeta^{-1})$.

I

1. Calculer $\Phi_3^+(X)$ et $\Phi_5^+(X)$.
2. Déterminer le degré de $\Phi_p^+(X)$.
3. Démontrer qu'on a $\Phi_p(X) = X^{(p-1)/2}\Phi_p^+(X + 1/X)$.
4. En déduire que $\Phi_p^+(X) \in \mathbf{Z}[X]$. (On pourra considérer $\Phi_p^+(X) = \sum_n a_n X^n$ et $n_0 = \mathrm{Max}\{n / a_n \notin \mathbf{Z}\}$.)
5. Démontrer que $\Phi_p^+(X)$ est irréductible sur $\mathbf{Q}$.

II

Notons $\mathbf{Q}(\mu_p)$ le p-ème corps cyclotomique, *i.e.* le corps de décomposition de Φ_p dans $\mathbf{C}$. Fixons $\zeta_0 \in \mu_p$. Soit $\mathbf{Q}(\zeta_0 + \zeta_0^{-1})$ un corps de rupture de Φ_p^+ dans $\mathbf{C}$.

1. Quel est le degré de $\mathbf{Q}(\zeta_0 + \zeta_0^{-1})$ sur $\mathbf{Q}$?
2. Combien y a-t-il de plongements $\sigma : \mathbf{Q}(\zeta_0 + \zeta_0^{-1}) \to \mathbf{C}$?
3. Quelles sont alors les valeurs possibles de $\sigma(\zeta_0 + \zeta_0^{-1})$?
4. Démontrer que σ est alors à valeurs dans $\mathbf{R}$.
5. Démontrer que $\mathbf{Q}(\zeta_0 + \zeta_0^{-1})$ est contenu dans $\mathbf{Q}(\mu_p)$.

III

On rappelle que l'extension $\mathbf{Q}(\mu_p)|\mathbf{Q}$ est galoisienne et que l'application $(\mathbf{Z}/p\mathbf{Z})^* \to \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ qui à $a + p\mathbf{Z}$ associe σ_a est un isomorphisme de groupes, où σ_a est caractérisé par $\sigma_a(\zeta) = \zeta^a$ ($\zeta \in \mu_p$). Notons $\mathbf{Q}(\mu_p)^+$ le sous-corps de $\mathbf{Q}(\mu_p)$ formé par les éléments invariants par $\{\sigma_1, \sigma_{-1}\}$.

1. Quel est le degré de l'extension $\mathbf{Q}(\mu_p)^+|\mathbf{Q}$?
2. Démontrer que $\mathbf{Q}(\mu_p)^+$ contient $\mathbf{Q}(\zeta_0 + \zeta_0^{-1})$, puis que $\mathbf{Q}(\zeta_0 + \zeta_0^{-1}) = \mathbf{Q}(\mu_p)^+$.
3. Démontrer que $\mathbf{Q}(\mu_p)^+$ est un corps de décomposition de $\Phi_p^+(X)$.
4. Démontrer que l'extension $\mathbf{Q}(\mu_p)^+|\mathbf{Q}$ est galoisienne.
5. Quel est le lien entre le groupe de Galois de cette extension et $(\mathbf{Z}/p\mathbf{Z})^*$?

IV

Soit q un nombre premier impair distinct de p. Le *symbole de Legendre* $\left(\frac{p}{q}\right)$ vaut par définition 1 si p est un carré modulo q (*i.e.* la classe $\tilde{p}$ de p modulo q s'écrit a^2 avec $a \in \mathbf{Z}/q\mathbf{Z}$) et -1 sinon. Soient P et $Q \in \mathbf{Z}[X]$ deux polynômes unitaires de degrés r et s respectivement. Notons $\mathrm{R}(P,Q) = \prod_{\alpha,\beta}(\alpha - \beta)$ (où α et β parcourent respectivement les racines de P et Q dans $\mathbf{C}$ comptées avec multiplicités) le résultant de ces polynômes. On note $\tilde{P}$ et $\tilde{Q}$ les classes dans $\mathbf{F}_q[X]$ de P et Q.

1. Démontrer que $\mathrm{R}(P,Q) = (-1)^{rs}\mathrm{R}(Q,P)$ et que la classe modulo q de $\mathrm{R}(P,Q)$ est $\mathrm{R}(\tilde{P},\tilde{Q})$.
2. Démontrer que $\tilde{\Phi}_q^+(X) = (X-2)^{(q-1)/2}$. En déduire que $\mathrm{R}(\tilde{\Phi}_q^+, \tilde{\Phi}_p^+) = \tilde{p}^{(q-1)/2}$.
3. Établir que $\left(\frac{p}{q}\right) \equiv p^{(q-1)/2} \pmod{q}$.
4. Démontrer que $\mathrm{R}(\Phi_q^+, \Phi_p^+)^2 = \prod_{\lambda\in\mu_q}\lambda^{-(p-1)/2}\Phi_p(\lambda)$. En déduire que $\mathrm{R}(\Phi_p^+, \Phi_q^+) \in \{-1, 1\}$.
5. Démontrer que $\mathrm{R}(\Phi_q^+, \Phi_p^+) = \left(\frac{p}{q}\right)$. En déduire la formule de Gauss (*loi de réciprocité quadratique*) :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$