Préparation à l'agrégation, algèbre

Devoir à la maison à rendre le 31 mars 2003

Exercice – Soit $P(X) = (X^2 + X + 1)^2 - 2X^2 \in \mathbb{Q}[X]$.

a) Montrer que P est irréductible.

b) Montrer que P admet exactement deux racines réelles, de module différent de 1, et deux racines non réelles u, v, de module 1.

c) En déduire que u et v sont des nombres algébriques de module 1 qui ne sont pas des racines de l'unité.

Problème – Soit p un nombre premier impair. On note $\mathbb{F}_p$ le corps à p éléments, 1_p son élément unité.

A

Soit f un polynôme unitaire de degré n à coefficients dans $\mathbb{F}_p$, sans racine multiple. On a donc une décomposition

$$f(X) = \prod_{1 \leq i \leq n} (X - \alpha_i)$$

dans le corps K de décomposition de f sur $\mathbb{F}_p$. On considère l'expression

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

1. Montrer que l'application $\alpha \mapsto \alpha^p$ permute les racines de f. Montrer que $D \in \mathbb{F}_p$.

2. On pose

$$\delta = \prod_{i<j} (\alpha_i - \alpha_j), \quad \text{d'où } D = \delta^2.$$

Montrer que $\delta^p = \pm\delta$, où le signe est la signature de la permutation $\alpha \mapsto \alpha^p$ des racines de f.

3. Soient r le nombre de facteurs irréductibles de f sur $\mathbb{F}_p$ et $n_1, ..., n_r$ leurs degrés. Montrer que $\alpha \mapsto \alpha^p$ permute circulairement les racines de chacun de ces facteurs; en déduire que le signe qui apparaît dans la question **2.** est

$$\prod (-1)^{n_i - 1} = (-1)^{n-r}.$$

Montrer que D est un carré dans $\mathbb{F}_p$ si et seulement si $n - r$ est pair.

4. Montrer qu'on a aussi

$$D = (-1)^{n(n-1)/2} \prod f'(\alpha_i).$$

On suppose que $f(X) = X^n - 1$ où $n = 2n' + 1$ est un entier impair non divisible par p. Montrer que $D = (-1)^{n'} n^n . 1_p$ et en déduire que $(-1)^{n'} n . 1_p$ est un carré dans $\mathbb{F}_p$ si et seulement si le nombre de facteurs irréductibles de $X^n - 1$ sur $\mathbb{F}_p$ est impair.

B

1. L'entier n étant premier avec p, montrer que les racines de $X^n - 1$ dans son corps de décomposition sur $\mathbb{F}_p$ forment un groupe cyclique d'ordre n. En utilisant la permutation $\alpha \mapsto \alpha^p$ de ces racines (voir **A 3.**), montrer que le nombre r des facteurs irréductibles de $X^n - 1$ sur $\mathbb{F}_p$ est égal au nombre de cycles de la permutation $x \mapsto px$ du groupe additif $\mathbb{Z}/n\mathbb{Z}$, et que le degré de ces polynômes est donné par la longueur des cycles. Expliciter le cas $p = 3, n = 16$.

2. On suppose que $n = q$, un nombre premier impair distinct de p. Soit e l'ordre de l'élément $p.1_q$ du groupe multiplicatif $\mathbb{F}_q^*$ du corps $\mathbb{F}_q$ à q éléments. Montrer que dans ce cas

$$r = 1 + \frac{q-1}{e}\,.$$

Montrer que l'élément $p.1_q$ du groupe $\mathbb{F}_q^*$ est un carré dans $\mathbb{F}_q$ si et seulement si $\frac{q-1}{e}$ est pair.

3. Posant $q = 2q' + 1$, montrer que l'entier $(-1)^{q'}q$ est un carré mod p si et seulement si l'entier p est un carré mod q; appliquant le critère d'Euler on obtient donc la *loi de réciprocité quadratique*.

4. On suppose maintenant que $n = \frac{p^2+1}{2}$. Montrer l'égalité des symboles de Legendre $(\frac{n}{p})$ et $(\frac{2}{p})$. Déterminer l'ordre de $p.1_n$ dans $(\mathbb{Z}/n\mathbb{Z})^*$, et montrer que dans ce cas $r = 1 + \frac{n-1}{4}$. Déduire de **A 4.** que

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}\,.$$

******