Examen Algèbre ENS 2009/2010

1 Exercice

Soient p un nombre premier, n un entier positif et $q = p^n$. On note $\mathbb{F}_q$ le corps fini à q éléments.

(a) On suppose $p > 2$. Montrer que x est un carré dans $\mathbb{F}_p^*$ si et seulement si $x^{\frac{p-1}{2}} = 1$. En déduire que -1 est un carré dans $\mathbb{F}_p^*$ si et seulement si $p \equiv 1 \mod 4$.

(b) Déterminer l'ensemble des nombres premiers p tels que le polynôme $X^2 + 1$ soit irréductible sur $\mathbb{F}_p$.

(c) On suppose de nouveau $p > 2$. Montrer que 8 divise $p^2 - 1$. En déduire que le polynôme $X^4 + 1$ n'est pas irréductible sur $\mathbb{F}_p$.

(d) Montrer que X^4+1 n'est pas irréductible sur $\mathbb{F}_2$ et déterminer l'ensemble des nombres premiers p tels que $X^4 + 1$ ait une racine dans $\mathbb{F}_p$.

(e) Montrer qu'il existe un polynôme irréductible dans $\mathbb{Z}[X]$ dont la réduction modulo p est réductible pour tout nombre premier p.

2 Exercice

Soit d un entier qui est produit de nombres premiers distincts. Soit A l'anneau $A := \mathbb{Z}[X]/(X^2 - d)\mathbb{Z}[X]$.

(a) Montrer que $A = \{a + b\sqrt{d}, a \in \mathbb{Z}, b \in \mathbb{Z}\}$ et que A est intègre.

(b) Pour $x = a + b\sqrt{d} \in A$, on définit la norme $N(x)$ de x par $N(x) = a^2 - b^2 d$. Montrer que pour tout x, y dans A, $N(xy) = N(x)N(y)$. Montrer que $x \in A^*$ si et seulement si $N(x) = \pm 1$.

(c) Soit $x \in A^*$. Montrer que $(x, -x, x^{-1}, -x^{-1})$ sont des unités et que si $x \neq \pm 1$ il existe un seul d'entre eux qui est > 1 et que ce nombre est de la forme $a + b\sqrt{d}$ avec $a > 0$ et $b > 0$.

(d) Soit $x_1 := a_1 + b_1\sqrt{d} \in A^*$ avec $a_1 > 0$ et $b_1 > 0$. On pose

$$a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n.$$

Montrer que la suite b_n est strictement croissante.

(e) Montrer que les seules racines de l'unité de A^* sont ± 1.

(f) Soit G le sous-groupe de A^* formé des unités positives. Soit $\psi : G \to \mathbb{R}^2$ l'application

$$x = a + b\sqrt{d} \mapsto \psi(x) := (\log|a + b\sqrt{d}|, \log|a - b\sqrt{d}|).$$

Montrer que ψ est un morphisme de groupes (avec $\mathbb{R}^2$ muni de l'addition) et que l'image de ψ est contenu dans la droite D d'équation $x + y = 0$.

(g)Montrer que $\psi(G)$ est discret dans D et en déduire que G est un $\mathbb{Z}$-module libre de rang 0 ou 1.

(h) Si $G = \{(a_1 + b_1\sqrt{d})^n, n \in \mathbb{Z}\}$ avec $a_1 > 0$, $b_1 > 0$, on dit que $x := a_1 + b_1\sqrt{d}$ est l'unité fondamentale. En utilisant (d) décrire un algorithme pour calculer l'unité fondamentale. Montrer que $G = \mathbb{Z}$ pour $d = 3, 7, 11$ et déterminer l'unité fondamentale pour ces valeurs.

Remarque: On peut montrer que $G = \mathbb{Z}$ pour tout d.

3 Exercice

Soit A un anneau commutatif noethérien. Si I est un idéal de A, on pose $R(I) := \{a \in A, \exists n \in \mathbb{N}, a^n \in I\}$.

(a) Montrer que $R(I)$ est un idéal et qu'il existe un entier naturel n tel que $R(I)^n \subset I$.

(b) On dit qu'un idéal I est réductible si il existe deux idéaux J et K distincts de I tels que $I = J \cap K$. Dans le cas contraire, on dit que I est irréductible. Montrer que tout idéal premier est irréductible et que tout idéal est l'intersection d'un nombre fini d'idéaux irréductibles.

(c) Pour tout $a \in A$ on note $\phi_a : A \to A$ l'application définie par $\phi_a(x) = ax$. On suppose qu'il existe $a \in A$ non nilpotent tel que ϕ_a ne soit pas injective. En considérant les noyaux et les images de ϕ_{a^n} montrer que (0) est un idéal réductible.

(d) Montrer que si (0) est irréductible $R((0))$ est premier.

(e) Montrer que si I est un idéal propre irréductible $R(I)$ est premier.

(f) Montrer que l'on peut trouver des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ et des entiers $n_1, \ldots, n_r$ tels que

$$(0) = \mathfrak{p}_1^{n_1} \cap \cdots \cap \mathfrak{p}_r^{n_r}.$$

(g) On dit qu'un idéal premier de A est minimal si il ne contient strictement aucun idéal premier. Montrer qu'il existe dans A au plus un nombre fini d'idéaux premiers minimaux et que tout idéal premier contient un idéal premier minimal.

4 Exercice

Soit $\rho : G \to \mathrm{GL}(E)$ une représentation linéaire complexe de dimension finie d'un groupe fini G. Soit χ son caractère.

(1) Montrer que pour $g \in G$, $\rho(g) = Id_E$ si et seulement si $\chi(g) = \chi(1)$.

(2) On suppose de plus que ρ est fidèle (donc $Ker(\rho) = \{1\}$) et que χ prend t valeurs distinctes $a_1, \ldots, a_t$. On convient que $a_1 = \chi(1)$. On pose

$$A_j := \{x \in G | \chi(x) = a_i\}(\text{ pour } 1 \leq j \leq t$$

et on choisit $x_j \in A_j$ pour $1 \leq j \leq t$.

(2.a) Soit $M = (\chi^i(x_j))$ avec $0 \leq i \leq t-1$ et $1 \leq j \leq t$. Montrer que $det(M) \neq 0$.

(2.b) Soit ψ un caractère d'une représentation irréductible de G telle que ψ soit orthogonale à χ^i pour $0 \leq j \leq t-1$. Montrer que pour tout $1 \leq j \leq t$,

$$\sum_{x \in A_j} \psi(x) = 0.$$

(2.c) En déduire qu'il n'existe pas de tel caractère ψ (on pourra utiliser le 1). En conclure que toute représentation irréductible de G apparaît dans l'une des puissances $\rho^{\otimes i}$ pour $0 \leq i \leq t-1$.

(2.d) Donner un exemple avec $t = 2$ et un exemple avec $t = |G|$.