Université Claude Bernard Lyon 1

MASTER M1G

Algèbre

EXAMEN

8 Janvier 2016

Durée : 3 heures

Le mathématicien se situe à la médiane de la liberté infinie et de la contrainte implacable. A ce titre, il incarne de façon emblématique la condition humaine. Bref, toutes vos idées sont les bienvenues, à condition qu'elles soient bien rédigées.

Exercice 1

Montrer que le polynôme $X^2 + Y^2 - 1$ est irréductible dans $\mathbb{C}[X, Y]$.

Exercice 2. *Question de cours*

Montrer que si P est un polynôme irréductible de degré n sur un corps $\mathbb{K}$, et si $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré m premier avec n, alors P reste irréductible sur $\mathbb{L}$.

Exercice 3.

1. Soit $A = \mathbb{Z}[i\sqrt{3}]$ le sous-anneau (unitaire) de $\mathbb{C}$ engendré par $i\sqrt{3}$. Montrer, à l'aide d'un isomorphisme bien conduit, que $A/(2)$ n'est pas intègre.
2. En déduire que l'anneau A n'est pas factoriel.

Problème.

Soit p un nombre premier congru à -3 modulo 8. Le but du problème est de montrer que l'anneau $C := \mathbb{Z}[\alpha]$, avec $\alpha = \sqrt{2p}$, n'est pas principal.

A.

1. Montrer que $\alpha \notin \mathbb{Q}$.
2. Montrer que tout élément de C s'écrit *de façon unique*, sous la forme $a + b\alpha$, avec $a, b \in \mathbb{Z}$.
3. Soit $\mathbb{K}$ le corps des fractions de C. Montrer que tout élément de $\mathbb{K}$ s'écrit *de façon unique*, sous la forme $x + y\alpha$, avec $x, y \in \mathbb{Q}$.
4. Soit N l'application
$$N : \mathbb{K} \to \mathbb{Q}^+,\ x + y\alpha \mapsto |x^2 - 2py^2|.$$
Montrer les propriétés suivantes :
   (a) pour tout k, k' de K, on a $N(kk') = N(k)N(k')$,

(b) pour tout c de C, on a $N(c) \in \mathbb{N}$, avec $N(c) = 0$ si et seulement si $c = 0$,

(c) le groupe des unités de C est donné par $C^* := \{u \in C,\ N(u) = 1\}$.

B.

On suppose ici que p est tel que C soit *principal*.

1. Montrer alors que tout élément k de $\mathbb{K}$ peut s'écrire sous la forme $k = \frac{\gamma}{\beta}$, avec γ et β dans C, sans diviseur commun non unitaire.
2. Montrer qu'il existe u et v dans C tels que $u\gamma - v\beta = 1$.
3. En déduire que, pour tout k de $\mathbb{K}$, $k \notin C$, il existe u et v dans C tels que

$$0 < N(ku - v) < 1.$$

C.

On pose ici $k := \frac{\alpha}{2}$.

1. Montrer que $k \in \mathbb{K}$, avec $k \notin C$.
2. On pose donc

$$u = x + y\alpha,\ v = z + t\alpha,\ \text{avec } 0 < N(ku - v) < 1.,$$

avec $x, y, z, t \in \mathbb{Z}$. Montrer que l'on a alors

$$0 < \left|2(py - z)^2 - p(x - 2t)^2\right| < 2.$$

3. En déduire que $\bar{2}\bar{z}^2 = \pm\bar{1}$.

D.

On note $\left(\frac{a}{p}\right)$ le *symbole de Legendre* de l'entier a modulo p. On pourra admettre [1] que

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

1. Montrer l'égalité

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

2. En déduire que 2 et -2 ne sont pas des carrés modulo p.
   On rappelle que, par hypothèses, p est congru à -3 modulo 8.
3. En déduire que C n'est pas principal.

1. Voir l'examen 2015 pour une preuve classique, mais non moins élégante.