Université Claude Bernard Lyon 1

MASTER M1-G

Algèbre

EXAMEN

9 Janvier 2015

Durée : 3 heures

Chaque fois que la factorialité intervient, signale-le sur ta copie et gagne des points s'miles ! L'offre est aussi valable pour toutes les propriétés du cours qui jouent un rôle dans la résolution des questions et pour la pertinence des hypothèses.

Exercice clef

Après avoir décrit brièvement le groupe $(\mathbb{Z}/8\mathbb{Z})^*$, montrer que si a est un entier impair, alors $a^2 \equiv 1$ modulo 8.

Problème 1. Une équation de Mordell

On propose de montrer que si les entiers x, y vérifient

$$y^2 + 11 = x^3, \tag{1}$$

alors (x, y) est soit $(3, \pm 4)$ soit $(15, \pm 58)$ qui saute aux yeux.

On note dans la suite α le nombre complexe $\frac{1+i\sqrt{11}}{2}$ et A l'anneau $\mathbb{Z}[\alpha]$.

A. *Etude de l'anneau A*

On va dans un premier temps étudier les propriétés de base de l'anneau A que l'on munit, par restriction, de la norme complexe $N(z) := z\bar{z}$.

1. Montrer que $\alpha^2 - \alpha + 3 = 0$ et en déduire $\mathbb{Z}[\alpha] = \{a + b\alpha,\ a,\ b \in \mathbb{Z}\}$.
2. Montrer que $N(a+b\alpha) = a^2 + ab + 3b^2$ et en déduire que les unités de l'anneau A sont ± 1.
3. On veut montrer que A est un anneau euclidien. On fixe $z = x + iy \in \mathbb{C}$.
   (a) Montrer qu'il existe deux entiers n et m tels que
   $$\left|\frac{2y}{\sqrt{11}} - n\right| \leq \frac{1}{2},\ \left|x - m - \frac{n}{2}\right| \leq \frac{1}{2}.$$
   (b) Montrer l'égalité $|z - m - n\alpha|^2 = (x - m - \frac{n}{2})^2 + \frac{11}{4}(\frac{2y}{\sqrt{11}} - n)^2$.
   (c) En déduire que A est un anneau euclidien.
4. Montrer que 2 et $-1 + 2\alpha$ sont premiers dans A.

B. *Etude préliminaire de l'équation*

Nous allons ici éliminer quelques cas fâcheux dans la résolution de l'équation. Le but de cette partie est de montrer que y ne peut être ni impair, ni multiple de 11, puis d'en déduire que $y + i\sqrt{11}$ et $y - i\sqrt{11}$ sont premiers entre eux dans A. On suppose donc que (x, y) est une solution de l'équation diophantienne (1).

1. Montrer que si y est impair, alors x est pair. En déduire une contradiction, en utilisant l'exercice clef.
2. Montrer que si 11 divise y, alors 11 divise x. En déduire une contradiction.
3. Soit δ premier dans A qui divise $y + i\sqrt{11}$ et $y - i\sqrt{11}$ dans A. Montrer que $N(\delta)$ divise 44 dans $\mathbb{N}$.
4. On admettra dans la suite cette information donnée par le logiciel SAGE, en quelques millièmes de seconde, que si $N(a + b\alpha)$ divise 44, et distinct de 1, alors $a + b\alpha = \pm 2$, $\pm(-1 + 2\alpha)$, ou $\pm 2(-1 + 2\alpha)$. Montrer alors que δ est un premier associé à 2 ou à $-1 + 2\alpha$ et déduire une contradiction.
5. Déduire que $y + i\sqrt{11}$ et $y - i\sqrt{11}$ sont premiers entre eux dans A.

C. *Résolution de l'équation*

On suppose donc encore ici que (x, y) est une solution de l'équation diophantienne (1).

1. Montrer que $y + i\sqrt{11}$ est un cube de A.
   Suggestion : on pourra remarquer que -1 est un cube.
2. Soit a et b deux entiers tels que $y + i\sqrt{11} = (a + b\alpha)^3$. Montrer que $b = \pm 1$ ou ± 2.
3. Montrer que $b = 1$ et $b = -2$ ne donnent pas de solution.
4. Montrer que $b = -1$ et $b = 2$ donnent les solutions attendues.

Problème 2. Un cas particulier de la réciprocité quadratique

Soit $q = p^k$, avec p premier impair. Le but du problème est de prouver que 2 est un carré de $\mathbb{F}_q$ si et seulement si $q \equiv \pm 1$ modulo 8, et ce, tout en testant élégamment vos connaissances et votre savoir-faire.

A. *Etude du polynôme $X^4 + 1$ sur $\mathbb{F}_q$*

Le but de cette partie est de montrer que le polynôme $X^4 + 1$ est toujours réductible sur $\mathbb{F}_q$. On considère une racine α de $X^4 + 1$ dans une extension de $\mathbb{F}_q$.

1. Montrer que $X^4 + 1$ ne possède pas de racine multiple (dans toute extension de $\mathbb{F}_q$).
2. Montrer que l'ensemble des racines de $X^4 + 1$ est $\{\alpha, -\alpha, \alpha^{-1}, -\alpha^{-1}\}$.
   Attention : la difficulté n'est pas de montrer qu'elles sont racines...
3. (a) Montrer, en utilisant l'exercice clef, que 8 divise l'ordre du groupe multiplicatif $\mathbb{F}_{q^2}^*$.
   (b) En déduire qu'il existe un élément α' d'ordre 8 dans $\mathbb{F}_{q^2}^*$.
   (c) Montrer alors que α' est racine de $X^4 + 1$.
4. En déduire que α est dans $\mathbb{F}_{q^2}$.
5. Conclure que $X^4 + 1$ est réductible sur $\mathbb{F}_q$.
   Suggestion : pense à ton corps !

B. *Implication « 2 est un carré de $\mathbb{F}_q \Longrightarrow q \equiv \pm 1$ modulo 8 »*

On considère encore une fois que α est une racine de $X^4 + 1$.

1. En remarquant que $\alpha^5 = -\alpha$, montrer que l'ensemble des racines de $X^4 + 1$ peut aussi s'écrire $\{\alpha, \alpha^3, \alpha^5, \alpha^{-1}\}$. En déduire que α^q ne peut être égal qu'à une de ces quatre valeurs.
2. Montrer que si $\alpha^q = \alpha^n$ pour un entier n, alors $q \equiv n$ modulo 8.
3. On pose maintenant $\beta = \alpha + \alpha^{-1}$. Montrer que $\beta^2 = 2$. Quelle est l'autre racine de $X^2 = 2$?
4. On suppose maintenant que 2 est un carré de $\mathbb{F}_q$. Montrer alors que $\beta^q = \beta$.
5. En déduire dans ce cas que $q \equiv \pm 1$ modulo 8.

C. *Implication « $q \equiv \pm 1$ modulo 8 $\Longrightarrow$ 2 est un carré de $\mathbb{F}_q$ »*

1. Montrer comment le raisonnement de la partie B s'inverse pour donner la réciproque.
2. En utilisant les notations standard du symbole de Legendre, montrer l'égalité suivante, où p désigne un nombre premier impair,

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

L'intention au départ était de mettre un portrait de l'illustre Kim Jung Un. Mais, après des cybermenaces de la Corée du Nord, nous avons préféré mettre le portrait de cet homme, non moins illustre, et à l'origine de ces deux problèmes. Sauras-tu le reconnaître ?