Université Claude Bernard Lyon 1

MASTER M1G

Algèbre

Fiche TD 4

Exercice 1 *Symbole de Legendre*
Soit p un nombre premier impair et a un élément de $\mathbb{F}_p^*$. Montrer que l'on a

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^*, \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^*. \end{cases}$$

Soluce :

Considérons les morphismes de groupes $\chi : \mathbb{F}_p^* \to \mathbb{F}_p^*$ et $\lambda : \mathbb{F}_p^* \to \mathbb{F}_p^*$, donnés respectivement par $x \mapsto x^2$ et $x \mapsto x^{(p-1)/2}$. D'après le théorème de Lagrange ou le petit théorème de Fermat, le morphisme composé $\lambda \circ \chi = \chi \circ \lambda : x \mapsto x^{p-1}$ est trivial. En particulier, $\lambda(a) = a^{(p-1)/2}$ admet pour carré 1 donc, par intégrité de $\mathbb{F}_p$, vaut ± 1.

On a une suite de groupes :

$$1 \longrightarrow \{-1, 1\} \longrightarrow \mathbb{F}_p^* \xrightarrow{\chi} \mathbb{F}_p^* \xrightarrow{\lambda} \{-1, 1\} \longrightarrow 1.$$

Vu que $\lambda(a)$ vaut -1 ou 1, il s'agit de montrer que a appartient à $\operatorname{Im}\chi$ si et seulement si a appartient à $\ker\lambda$. Autrement dit, que $\operatorname{Im}\chi = \ker\lambda$, ou encore que la suite est exacte. Mais l'on a déjà vu l'inclusion : $\operatorname{Im}\chi \subset \ker\lambda$. De plus, on a : $|\operatorname{Im}\chi| = |\mathbb{F}_q^*|/|\ker\chi| = (p-1)/2$ et $|\ker\lambda| \leq (p-1)/2$ puisque $\ker\lambda$ est l'ensemble des racines du polynôme $x^{(p-1)/2} - 1$ sur un corps (commutatif). On peut conclure l'égalité $\operatorname{Im}\chi = \ker\lambda$.

Exercice 2 *Sous-anneaux quadratiques de* $\mathbb{C}$
On posera successivement $\alpha = i$, $i\sqrt{2}$, $i\sqrt{3}$, $\frac{1+i\sqrt{3}}{2}$, $\frac{1+i\sqrt{5}}{2}$, $\frac{1+i\sqrt{7}}{2}$, $\frac{1+i\sqrt{19}}{2}$.

1. Montrer que l'anneau $\mathbb{Z}[\alpha]$ est stable par conjugaison.
2. Trouver un polynôme de degré 2 à coefficients entiers qui annule α. Montrer que tout élément de $\mathbb{Z}[\alpha]$ s'écrit de façon unique sous la forme $x + y\alpha$, avec $x, y \in \mathbb{Z}$.
   Apprendre en s'amusant : donner une représentation matricielle de $x+y\alpha$ et utiliser Cayley-Hamilton.
3. Calculer la norme d'un élément de la forme $x + y\alpha$ avec x, y réels. En déduire que la norme définit une application multiplicative de $\mathbb{Z}[\alpha]$ dans $\mathbb{N}$.
4. Montrer que les éléments inversibles de $\mathbb{Z}[\alpha]$ sont les éléments de norme 1. Décrire le groupe multiplicatif $\mathbb{Z}[\alpha]^*$.
   SI un élément est inversible, il vérifie $\overline{z}z = 1$. Il faut tout de même utiliser que $\mathbb{Z}[\alpha]$ est stable par conjugaison !

5. Soit z dans $\mathbb{C}$, que l'on décompose en $z = x + y\alpha$, avec $x, y \in \mathbb{R}$. Pour quels α dans la liste existe-t-il toujours $z_0 = x_0 + y_0\alpha \in \mathbb{Z}[\alpha]$ tel que $N(z - z_0) < 1$. Montrer que dans ce cas, l'anneau $\mathbb{Z}[\alpha]$ est euclidien.

Exercice 3 *Anneaux non factoriels*

1. Montrer que l'anneau $\mathbb{C}[X, Y, Z]/(XZ - Y^2)$ est non factoriel. Par exemple, en montrant qu'il est isomorphe au sous-anneau $\mathbb{C}[T^2, T^3]$ de $\mathbb{C}[T]$.
2. Montrer que l'anneau $A := \mathbb{Z}[i\sqrt{5}]$ est non factoriel. On pourra remarquer que $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 2 \times 3$.
   On pourra se référer au document sur les anneaux non factoriels distribué en TD.

Exercice 4 *Lemme préliminaire pour certaines équations diophantiennes* Soit A un anneau factoriel. On suppose que x, y sont premiers entre eux et qu'il existe z dans A tel que

$$xy = z^k$$

1. Montrer qu'il existe u et v dans A^* ainsi que x_0, y_0 dans A tels que

   $$x = ux_0^k,\ y = vy_0^k.$$

   Interpréter les hypothèses en termes de valuation.
2. On suppose que A^* est d'ordre fini premier avec k. Montrer alors que qu'il existe x_1, y_1 dans A tels que

   $$x = x_1^k,\ y = y_1^k.$$

   Pourquoi le morphisme $w \mapsto w^k$ de A^* dans lui-même est-il injectif ? Surjectif ?

Exercice 5 *Une équation de Mordell*
On veut montrer que les solutions de l'équation diophantienne

$$y^2 = x^3 - 2$$

sont $(3, \pm 5)$. On suppose dans la suite que (x, y) est un couple de solutions entières de l'équation.

1. Montrer que $y + i\sqrt{2}$ et $y - i\sqrt{2}$ dans l'anneau factoriel $A := \mathbb{Z}[i\sqrt{2}]$.
   Prendre un diviseur commun d, qu'il ne coûte pas plus cher de choisir premier. Montrer que forcément d est associé à $i\sqrt{2}$, puis, on en déduit que 2 divise y et x. Ceci aboutit facilement à une contradiction.
2. En déduire que $y + i\sqrt{2}$ est un cube de A et conclure. *Quelles sont les unités de A ?*

Exercice 6 *Une autre équation de Mordell*
Montrer que si les entiers x, y vérifient

$$y^2 + 4 = x^3,$$

alors $(x, y) = (2, \pm 2)$ ou $(5, \pm 11)$.

Soluce

On travaille sur l'anneau euclidien (donc factoriel) $\mathbb{Z}[i]$.

$$x^3 = (y + 2i)(y - 2i). \ (*)$$

Nous allons montrer que ceci implique que les deux facteurs du membre de droite sont des cubes de $\mathbb{Z}[i]$. Montrons tout d'abord que ceci nous mènera avec puissance et élégance à la solution de l'énoncé. Supposons donc

$$y + 2i = (m + ni)^3, m, n \in \mathbb{Z}.$$

On obtient alors $y = m(m^2 - 3n^2)$, $2 = n(3m^2 - n^2)$. La seconde équation donne $n = \pm 1$ ou $n = \pm 2$.
On obtient cas par cas les solutions suivantes $(n, m) = (1, \pm 1)$, ou $(-2, \pm 1)$. Le premier cas donne $(x, y) = (2, \pm 2)$ et le second $(5, \pm 11)$.

Reste à montrer que $y + 2i$ et $y - 2i$ sont des cubes. En fait, par (*), il suffit de le montrer pour un des deux.
L'équation $y^2 + 4 = x^3$ quotientée dans $\mathbb{Z}/2\mathbb{Z}$ montre que x et y sont de même parité.

1er Cas. x et y sont impairs. Montrons que $y + 2i$ et $y - 2i$ sont premiers entre eux dans $\mathbb{Z}[i]$.
Soit d un diviseur commun à $(y + 2i)$ et $(y - 2i)$. Alors d divise $4i$. Donc, dans $\mathbb{Z}$, $N(d)$ divise 16 et $N(y+2i) = y^2+4$ qui est impair et ainsi $N(d) = 1$, ce qui fait de d une unité. Il vient que $y+2i$ et $y-2i$ sont bien premiers entre eux et donc l'équation montre que ce sont des cubes à unité près dans $\mathbb{Z}[i]$. Mais les unités de $\mathbb{Z}[i]$ sont elles-mêmes des cubes (ce sont les racines quatrièmes de l'unité et 3 est inversible dans $\mathbb{Z}/4\mathbb{Z}$), et donc notre assertion est vérifiée dans ce cas.

2ème cas. On suppose maintenant que x et y sont tous deux pairs. On pose $x = 2t$ et $y = 2z$, de sorte que

$$z^2 + 1 = 2t^3.$$

ce qui donne que z est impair et regardant cette équation modulo 2 et t est impair, en la regardant modulo 4. Donc, $z + i$ est divisible par $(1 + i)$ dans $\mathbb{Z}[i]$ et de même, $z - i$ est divisible par $(1 + i)$. D'où

$$-it^3 = \frac{z + i}{1 + i}\frac{z - i}{1 + i}.$$

Ces deux facteurs sont de plus premiers entre eux dans $\mathbb{Z}[i]$, puisque si d est un diviseur commun, alors, d divise leur différence $\frac{2i}{1+i}$. Ce qui donne $N(d)$ divise $N(\frac{2i}{1+i}) = 2$. Or, comme d divise t^3, $N(d)$ divise aussi $N(t^3) = t^6$ qui est impair. Donc d est une unité et on conclut comme dans le premier cas que $\frac{z+i}{1+i}$ est un cube, puis que $y + 2i = 2(z + i) = i^3(1 + i)^3\frac{z+i}{1+i}$ en est un aussi.