ÉNS Lyon — Algèbre 1
L3 — 2010–2011

DM 2

L'anneau $\mathbb{Z}[i\sqrt{2}]$.

On considère l'anneau $\mathbb{Z}[i\sqrt{2}] = \{a + bi\sqrt{2}\,;\ a, b \in \mathbb{Z}\}$, sur lequel on définit une application norme, N, donnée par

$$N(a + bi\sqrt{2}) = a^2 + 2b^2 \in \mathbb{N}.$$

1. Vérifier que l'application N est multiplicative.

Réponse. Soit $z \in \mathbb{Z}[i\sqrt{2}]$; notons $\bar{z}$ son complexe conjugué. Alors $\bar{z} \in \mathbb{Z}[i\sqrt{2}]$, et la relation $N(z) = z\bar{z}$ montre la multiplicativité de N.

2. Déterminer les éléments inversibles de l'anneau $\mathbb{Z}[i\sqrt{2}]$.

Réponse. Montrons d'abord qu'un élément $z \in \mathbb{Z}[i\sqrt{2}]$ est inversible si et seulement si $N(z) = 1$. En effet, si z est inversible dans $\mathbb{Z}[i\sqrt{2}]$, il existe $y \in \mathbb{Z}[i\sqrt{2}]$ tel que $zy = 1$, d'où $N(z)N(y) = 1$ par multiplicativité de N. Alors, $N(z)$ est inversible dans $\mathbb{Z}$. Puisque $N(z) \in \mathbb{N}$, cela entraîne $N(z) = 1$. Réciproquement, si $N(z) = 1$, alors z est inversible d'inverse $\bar{z} \in \mathbb{Z}[i\sqrt{2}]$.

Or la relation $a^2 + 2b^2 = 1$, avec $a, b \in \mathbb{Z}$, entraîne $a = \pm 1$ et $b = 0$.

Puisque 1 et -1 sont clairement inversibles dans $\mathbb{Z}[i\sqrt{2}]$, ce sont donc les seuls inversibles de l'anneau $\mathbb{Z}[i\sqrt{2}]$.

3. Montrer que l'anneau $\mathbb{Z}[i\sqrt{2}]$ est euclidien pour la norme, c'est-à-dire que l'application $N : \mathbb{Z}[i\sqrt{2}]\backslash\{0\} \to \mathbb{N}$ est un stathme euclidien.

Réponse. Pour montrer que l'anneau $\mathbb{Z}[i\sqrt{2}]$ est euclidien pour la norme, on va s'inspirer de l'exercice 12 du TD 7, sur l'anneau des entiers $\mathbb{Z}[i]$. Il suffit de montrer que, pour tout couple $(a, b) \in \mathbb{Z}[i\sqrt{2}]$ avec $b \neq 0$, le quotient $\dfrac{a}{b} \in \mathbb{C}$ est à distance inférieure à 1 d'un élément $q \in \mathbb{Z}[i\sqrt{2}]$.

En effet, on a les équivalences suivantes :

$$\begin{aligned}
\exists q, r \in \mathbb{Z}[i\sqrt{2}]\ a = bq + r \text{ et } N(r) < N(b) &\Leftrightarrow \exists q, r \in \mathbb{Z}[i\sqrt{2}]\ :\ \tfrac{a}{b} - q = \tfrac{r}{b} \text{ et } N(r) < N(b) \\
&\Leftrightarrow \exists q, r \in \mathbb{Z}[i\sqrt{2}]\ :\ \tfrac{a}{b} - q = \tfrac{r}{b}\left|\tfrac{r}{b}\right| < 1 \\
&\Leftrightarrow \exists q \in \mathbb{Z}[i\sqrt{2}]\ :\ \left|\tfrac{a}{b} - q\right| < 1.
\end{aligned}$$

Or tout nombre complexe $z = x + i\sqrt{2}y \in \mathbb{C}$ est bien à une distance inférieure à 1 d'un élément de $\mathbb{Z}[i\sqrt{2}]$. En effet, si x_0 et y_0 sont deux entiers tels que $|x - x_0| \leq \frac{1}{2}$ et $|y - y_0| \leq \frac{1}{2}$ (ces entiers existent bien, par exemple en prenant la partie entière inférieure ou supérieure), on a, en posant $z_0 = x_0 + i\sqrt{2}y_0 \in \mathbb{Z}[i\sqrt{2}]$:

$$N(z - z_0) = (x - x_0)^2 + 2(y - y_0)^2 \leq \frac{1}{4} + \frac{1}{2} < 1,$$

c'est-à-dire $|z - z'| < 1$.

L'équation diophantienne $x^2 + 2 = y^3$.

On souhaite montrer que les seuls couples d'entiers $(x, y) \in \mathbb{Z}^2$ tels que $x^2 + 2 = y^3$ sont les couples $(\pm 5, 3)$.

4. Dans l'anneau $\mathbb{Z}[i\sqrt{2}]$, montrer que l'élément $i\sqrt{2}$ est irréductible.

Réponse.

Solution 1. On remarque que $N(i\sqrt{2}) = 2$. Puisque 2 est premier dans $\mathbb{Z}$ et que l'application N est multiplicative, cela implique que $i\sqrt{2}$ est irréductible dans $\mathbb{Z}[i\sqrt{2}]$. En effet, si $i\sqrt{2} = xy$ dans $\mathbb{Z}[i\sqrt{2}]$, alors $2 = N(a)N(b)$, d'où $N(a) = 1$ ou $N(b) = 1$, c'est-à-dire, a ou b est inversible d'après la question 2.

Solution 2. L'application $\mathbb{Z}[i\sqrt{2}] \to \mathbb{Z}/2\mathbb{Z}$ donnée par $a + i\sqrt{2}b \mapsto (a \bmod 2)$ est un homomorphisme de groupes surjectif, de noyau $\mathfrak{p} = (i\sqrt{2})\mathbb{Z}[i\sqrt{2}]$. Elle induit donc un isomorphisme $\mathbb{Z}[i\sqrt{2}]/(i\sqrt{2})\mathbb{Z}[i\sqrt{2}] \simeq \mathbb{Z}/2\mathbb{Z}$. Puisque l'anneau $\mathbb{Z}/2\mathbb{Z}$ est intègre, cela montre que l'idéal engendré par $i\sqrt{2}$ est premier. Puisque l'anneau $\mathbb{Z}[i\sqrt{2}]$ est principal car euclidien, l'élément $i\sqrt{2}$ est donc irréductible.

5. Soit (x, y) une solution de l'équation $X^2 + 2 = Y^3$. Soit $\mathfrak{q}$ l'idéal de $\mathbb{Z}[i\sqrt{2}]$ engendré par les éléments $x + i\sqrt{2}$ et $x - i\sqrt{2}$.

a. **Montrer que l'idéal $\mathfrak{q}$ contient $2i\sqrt{2}$.**
Réponse. L'idéal $\mathfrak{q}$ contient la somme $x + i\sqrt{2} - (x - i\sqrt{2}) = 2i\sqrt{2}$.

b. **En déduire qu'il existe un entier m, avec $0 \leq m \leq 3$, tel que l'idéal $\mathfrak{q}$ est engendré par $(i\sqrt{2})^m$.**
Réponse. Notons $\alpha = i\sqrt{2}$. Puisque l'anneau $\mathbb{Z}[i\sqrt{2}]$ est principal, soit β un générateur de $\mathfrak{q}$. Comme $2i\sqrt{2} = 3$, l'idéal $\mathfrak{q}$ contient α^3, d'après la question précédente. Il existe donc $a \in \mathbb{Z}[i\sqrt{2}]$ tel que $\alpha^3 = \beta a$.
Si $\mathfrak{q} \neq \mathbb{Z}[i\sqrt{2}]$, l'élément β n'est pas inversible, et donc, par factorialité de l'anneau $\mathbb{Z}[i\sqrt{2}]$ (unicité de la décomposition en produit d'irréductibles), β est associé soit à α, soit à α^2, soit à α^3. C'est-à-dire, l'idéal $\mathfrak{q}$ est engendré par α ou α^2 ou α^3.
Si $\mathfrak{q} = \mathbb{Z}[i\sqrt{2}]$, alors $\mathfrak{q}$ est engendré par $1 = \alpha^0$.
En résumé, l'idéal $\mathfrak{q}$ est engendré par $(i\sqrt{2})^m$ avec $0 \leq m \leq 3$.

c. **Montrer que le cas $m \neq 0$ est impossible.**
Pour cela, on pourra montrer l'implication : $m \neq 0 \Rightarrow y^3 \equiv 2 \bmod 4$.
Réponse. Si $m \neq 0$, alors $i\sqrt{2}$ divise $x + i\sqrt{2}$, c'est-à-dire, il existe des entiers $a, b \in \mathbb{Z}$ tels que

$$x + i\sqrt{2} = i\sqrt{2}(a + i\sqrt{2}b),$$

d'où $x = -2b$. Mais alors, $y^3 = 4b^2 + 2$, d'où $y^3 \equiv 2 \bmod 4$, ce qui est impossible : en effet, dans $\mathbb{Z}/4\mathbb{Z}$, les cubes valent 0, 1 ou 3. Donc le cas $m \neq 0$ est impossible.

d. **En déduire que les éléments $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$.**
Réponse. D'après la question précédente, l'idéal $\mathfrak{q}$ est l'anneau $\mathbb{Z}[i\sqrt{2}]$ tout entier. En particulier, il existe $u, v \in \mathbb{Z}[i\sqrt{2}]$ tels que $u(x + i\sqrt{2}) + v(x - i\sqrt{2}) = 1$.

Il s'agit d'une relation de Bezout. L'anneau $\mathbb{Z}[i\sqrt{2}]$ étant principal, cela montre que les éléments $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$.

e. **En considérant la factorisation de y^3 dans l'anneau $\mathbb{Z}[i\sqrt{2}]$, montrer alors que $x + i\sqrt{2}$ est un cube dans cet anneau.**

Réponse. Si $y = \epsilon \prod_{i\in I} p_i^{\alpha^i}$ est la décomposition de y en produit fini d'éléments irréductibles, avec $\epsilon = \pm 1$, on a $y^3 = \pm \prod_{i\in I} p_i^{3\alpha_i}$.

Or, on a aussi la factorisation $y^3 = (x + i\sqrt{2})(x - i\sqrt{2})$. D'après la question 2, ni $x + i\sqrt{2}$, ni $x - i\sqrt{2}$, ne sont inversibles. D'après la question précédente, ces éléments sont premiers entre eux. Il existe donc un sous-ensemble non vide J de I tel que $x + i\sqrt{2} = \pm \prod_{i\in J} p_i^{3\alpha_i}$. Puisque 1 et -1 sont des cubes, ceci montre que $x + i\sqrt{2}$ est un cube dans l'anneau $\mathbb{Z}[i\sqrt{2}]$.

f. **En déduire : $x = \pm 5$ et $y = 3$.**

Réponse. D'après la question précédente, il existe $a, b \in \mathbb{Z}$ tels que

$$x + i\sqrt{2} = (a + bi\sqrt{2})^3,$$

d'où

$$\begin{cases} x &= a^3 - 6ab^2 \\ 1 &= (3a^2 - 2b^2)b. \end{cases}$$

La seconde égalité donne successivement $b = \pm 1$ et $3a^2 - 2 = \pm 1$. Il vient donc $a = \pm 1$, d'où $x = \pm 5$ d'après la première égalité, et $y = 3$.

Les seules solutions entières (x, y) de l'équation $X^2 + 2 = Y^3$ sont donc les couples $(\pm 5, 3)$.

L'anneau $\mathbb{C}[X, Y]/(X^2 - Y^3)$.

Cet exercice est indépendant des exercices précédents.

6. Soit A un anneau factoriel ; on note Frac(A) son corps des fractions. Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ un polynôme de degré $n \geq 1$. Si $r = \frac{p}{q}$ est une racine de P dans Frac(A), avec p et q premiers entre eux dans A, montrer que p divise a_0 et q divise a_n.

Réponse. Si $r = \frac{p}{q}$ est racine du polynôme P, alors, en multipliant par q^n la relation $P(r) = 0$ on obtient :

$$a_n p^n + a_{n-1} p^{n-1} q + a_{n-2} p^{n-2} q^2 + \cdots + a_1 p q^{n-1} + a_0 q^n = 0.$$

D'une part, cela entraîne l'égalité $-a_0 q^n = p(a_n p^{n-1} + \cdots + a_1 q^{n-1})$. Puisque l'anneau A est factoriel, et comme p et q sont premiers entre eux, on en déduit que p divise a_0 par unicité de la décomposition en produit d'irréductibles.

D'autre part, on a aussi l'égalité $a_n p^n = -q(a_{n-1} p^{n-1} + \cdots + a_1 p q^{n-2})$, qui, de même, montre que q divise a_n.

7. Soit B un anneau intègre, et soit A un sous-anneau de B. On dit qu'un élément $b \in B$ est *entier* sur A s'il est racine d'un polynôme unitaire à

coefficients dans A. Un anneau intègre A est dit *intégralement clos* si les seuls éléments de Frac(A) entiers sur A sont les éléments de A.

Montrer qu'un anneau factoriel est intégralement clos, par exemple à l'aide de la question 6.

Réponse. Soit A un anneau factoriel. Soit $r \in \mathrm{Frac}(A)$ un élement entier sur A. Il existe donc un polynôme unitaire P, à coefficients dans A, tel que $P(r) = 0$. Puisque l'anneau A est factoriel, on peut écrire $r = \frac{p}{q}$ avec $p, q \in A$ premiers entre eux. D'après la question précédente, cela entraîne que q divise 1, c'est-à-dire q est inversible dans A. Donc r appartient à l'anneau A.
Réciproquement, il est clair que tout élément de A est entier sur A.
Les éléments de Frac(A) entiers sur A sont donc précisément les éléments de A, ce qu'il fallait démontrer.

8.Soit $A = \mathbb{C}[X,Y]/(X^2 - Y^3)$. On note x et y les projections de X et Y dans A.

a. **Montrer que l'anneau A est intègre.**

On pourra utiliser la question 6 pour montrer que le polynôme $X^2 - Y^3$ est irréductible dans $\mathbb{C}[X,Y] = \mathbb{C}[Y][X]$.

Réponse. Il s'agit de montrer que l'idéal engendré par $X^2 - Y^3$ est premier. Or l'anneau $\mathbb{C}[X,Y]$ est factoriel d'après le cours. Il suffit donc de montrer que le polynôme $X^2 - Y^3$ est irréductible dans $\mathbb{C}[X,Y]$. Voyant cet anneau comme $\mathbb{C}[Y][X]$, il s'agit d'un polynôme de degré 2 à coefficients dans $\mathbb{C}[Y]$. Ce polynôme est donc irréductible si et seulement s'il n'admet pas de racine dans le corps $\mathbb{C}(Y) = \mathrm{Frac}(\mathbb{C}[Y])$. En effet, puisqu'il est primitif, le polynôme $X^2 - Y^3$ est irréductible dans $\mathbb{C}[Y][X]$, si et seulement s'il est irréductible dans $\mathbb{C}(Y)[X]$, et donc si et seulement s'il n'a pas de racine dans le corps $\mathbb{C}(Y)$.

Maintenant, l'anneau $\mathbb{C}[Y]$ est factoriel d'après le cours ; on peut donc appliquer la question 6. Si $R = \frac{P}{Q} \in \mathbb{C}(Y)$ est racine du polynôme $X^2 - Y^3$, alors le polynôme Q divise 1 dans $\mathbb{C}[Y]$, il est donc inversible et $R \in \mathbb{C}[Y]$. En écrivant $R = \sum_{i=0}^{n} a_i Y^i$ avec $a_i \in \mathbb{C}$, on en déduit $(\sum_i a_i Y^i)^2 - Y^3 = 0$, ce qui est impossible par considération du degré : le degré de $(\sum_i a_i Y^i)^2$ est pair, tandis que celui de Y^3 est impair, ces deux polynômes ne peuvent donc pas être égaux.

b. **Montrer qu'il existe un morphisme d'anneaux ϕ de A dans $\mathbb{C}[T]$ tel que $\phi(x) = T^3$ et $\phi(y) = T^2$, et qui prolonge l'identité sur $\mathbb{C}$.**

Réponse. Puisque l'anneau $\mathbb{C}[T]$ est commutatif, d'après la propriété universelle des polynômes, il existe un unique morphisme d'anneaux ψ_0 de $\mathbb{C}[X]$ dans $\mathbb{C}[T]$ qui envoie X sur T^3 et qui prolonge le morphisme identité sur $\mathbb{C}$. En appliquant à nouveau cet argument à ψ_0, il existe un unique morphisme d'anneaux ψ de $\mathbb{C}[X][Y] = \mathbb{C}[X,Y]$ dans $\mathbb{C}[T]$ qui envoie Y sur T^2 et qui prolonge ψ_0.

Or l'idéal engendré par $X^2 - Y^3$ est clairement inclus dans le noyau de ψ. Donc ψ se factorise en un morphisme d'anneaux ϕ de A dans $\mathbb{C}[T]$, tel que $\phi(x) = T^3$ et $\phi(y) = T^2$, et qui prolonge l'identité sur $\mathbb{C}$.

c. **Montrer que l'application ϕ est injective et que son image est le sous-anneau $\mathbb{C}[T^2, T^3]$ de $\mathbb{C}[T]$.**

Pour montrer l'injectivité de ϕ, on pourra penser à l'exercice 2 du TD 8.

Réponse. Avec les notations de la réponse précédente, il suffit de montrer que le noyau de l'homomorphisme ψ est l'idéal engendré par $(X^2 - Y^3)$ tout entier. Soit donc $P \in \mathbb{C}[X,Y] = \mathbb{C}[Y][X]$ un polynôme dans le noyau de ψ. Puisque le polynôme $X^2 - Y^3 \in \mathbb{C}[Y][X]$ est unitaire, on peut effectuer la division euclidienne de P : il existe deux polynômes $Q, R \in \mathbb{C}[Y][X]$ avec $\deg_X(R) < 2$ (degré en X) tels que

$$P(X) = (X^2 - Y^3)Q(X) + R(X) = (X^2 - Y^3)Q(X) + A(Y) + XB(Y),$$

en écrivant $R(X) = A(Y) + XB(Y)$, avec $A, B \in \mathbb{C}[Y]$. D'où $\psi(P) = A(T^2) + T^3B(T^2)$. Donc P est dans le noyau de ψ si et seulement si $A = B = 0$ dans $\mathbb{C}[Y]$ par considération des degrés (degrés en T uniquement pairs dans $A(T^2)$, et uniquement impairs dans $T^3B(T^2)$). Ceci montre que l'application ϕ est injective.

Clairement, puisque X et Y engendrent $\mathbb{C}[X,Y]$, l'image du morphisme ψ est $\mathbb{C}[T^2, T^3]$. Par factorisation par l'idéal $(X^2 - Y^3)$, cette image est inchangée. Donc l'image de ϕ est bien le sous-anneau $\mathbb{C}[T^2, T^3]$ de $\mathbb{C}[T]$.

d. **Montrer que le corps des fractions de A est isomorphe à $\mathbb{C}(T)$.**

Réponse. D'après ce qui précède, l'application ϕ induit un isomorphisme entre les anneaux A et $\mathbb{C}[T^2, T^3]$ qui sont intègres. En particulier, leurs corps de fractions sont isomorphes. Or le corps des fractions de $\mathbb{C}[T^2, T^3]$ est inclus dans le corps des fractions rationnelles $\mathbb{C}(T)$ et contient la fraction $\frac{T^3}{T^2} = T$: c'est donc le corps $\mathbb{C}(T)$.

e. **À l'aide de la question 7, montrer alors que l'anneau A n'est pas factoriel.**

Réponse. Il suffit de montrer que l'anneau $\mathbb{C}[T^2, T^3]$ n'est pas factoriel, puisque l'anneau A lui est isomorphe. Pour cela, nous allons montrer que l'anneau $\mathbb{C}[T^2, T^3]$ n'est pas intégralement clos. En effet, l'élément $T = \frac{T^3}{T^2} \in \mathbb{C}(T)$ n'appartient pas à $\mathbb{C}[T^2, T^3]$, mais est entier sur cet anneau puisqu'il annule le polynôme unitaire $X^2 - T^2$. On conclut grâce à la question 7.

f. **L'anneau A est-il noethérien ?**

Réponse. L'anneau A est noethérien, car quotient de l'anneau $\mathbb{C}[X,Y]$ qui est noethérien d'après le théorème de Hilbert.