TD6 : Anneaux euclidiens, principaux et factoriels

Diego Izquierdo

L'exercice 0 est à préparer avant la séance de TD. Pendant la séance, nous traiterons les exercices dans l'ordre suivant : 0, 2, 3, 10, 8. Si le temps le permet nous traiterons aussi l'exercice 4.

Exercice 0 (à préparer) : TD5
Terminer l'exercice 2 et faire l'exercice 6 du TD5.

Exercice 1 : Rappels sur les anneaux principaux

1. Soit k un corps. Rappeler pourquoi $k[X]$ est principal.

> **Indications :** Le stathme $k[X] \to \mathbb{N}, P \mapsto \deg P + 1$ montre que $k[X]$ est euclidien, donc principal.

2. Exhiber des idéaux non principaux dans $k[X,Y]$, $k[T^2,T^3]$, $\mathbb{Z}[X]$ et $\mathbb{Z}[i\sqrt{5}]$.

> **Indications :** Dans $k[X,Y]$, l'idéal (X,Y) n'est pas principal. Dans $k[T^2,T^3]$, l'idéal (T^2,T^3) n'est pas principal. Dans $\mathbb{Z}[X]$, l'idéal $(2,X)$ n'est pas principal. Dans $\mathbb{Z}[i\sqrt{5}]$, l'idéal $(2,1+i\sqrt{5})$ n'est pas principal.

Exercice 2 : Vrai ou faux ?
Soit A un anneau.

1. Un sous-anneau d'un anneau euclidien est factoriel.
2. L'anneau des nombres décimaux est euclidien.
3. Les groupes $\mathbb{Q}^\times$ et $(\mathbb{Z}/3\mathbb{Z}(X))^\times$ sont isomorphes.
4. Si A est factoriel, alors tout idéal premier non nul est maximal.
5. Le quotient d'un anneau factoriel par un idéal premier est factoriel.
6. Si A est un anneau factoriel et a et b sont des éléments non nuls de A, on a $(a,b) = (a \wedge b)$.
7. Si A est un anneau factoriel et a et b sont des éléments non nuls de A, on a $(a) \cap (b) = (a \vee b)$.
8. Si A est factoriel et si a et b sont deux éléments de A premiers entre eux, alors il existe un isomorphisme $A/(ab) \cong A/(a) \times A/(b)$.

Exercice 3 : Un exemple d'anneau non factoriel
Soit $A = \{P \in \mathbb{Q}[X] \mid P(0) \in \mathbb{Z}\}$. Montrer que A n'est pas factoriel.

Exercice 4 : Produits d'idéaux premiers
Considérons les anneaux $A = \mathbb{Z}[i\sqrt{11}]$ et $B = \mathbb{Z}[i\sqrt{13}]$.

1. Montrer que A et B ne sont pas des anneaux factoriels.

Indications : Dans A, on a l'égalité :

$$(1+i\sqrt{11})(1-i\sqrt{11}) = 2^2 \times 3.$$

Montrons que 2 est irréductible. Pour ce faire, considérons :

$$N : A \to \mathbb{Z}, z = a + bi\sqrt{11} \mapsto |z|^2 = a^2 + 11b^2.$$

Soient $x, y \in A$ tels que $xy = 2$. Alors $N(x)N(y) = N(2) = 4$. Comme l'équation $a^2 + 11b^2 = 2$ n'a pas de solutions entières, $N(x) = 1$ ou $N(y) = 1$. On en déduit que $x \in A^\times$ ou $y \in A^\times$. Donc 2 est bien irréductible. Comme 2 ne divise pas $1 + i\sqrt{11}$ dans A, l'anneau A n'est pas factoriel.

La preuve de la non factorialité de B est analogue en considérant l'égalité :

$$(1+i\sqrt{13})(1-i\sqrt{13}) = 2 \times 7.$$

2. Faire la liste des idéaux premiers de A qui contiennent l'idéal (2). En déduire que l'idéal (2) ne s'écrit pas comme produit d'idéaux premiers de A.

Indications : Les idéaux premiers de A contenant 2 sont en bijection avec les idéaux premiers de $A/(2)$. Or :

$$A/(2) \cong \mathbb{Z}[X]/(X^2 + 11, 2) \cong \mathbb{Z}/2\mathbb{Z}[X]/(X+1)^2.$$

L'anneau $\mathbb{Z}/2\mathbb{Z}[X]/(X+1)^2$ a une unique idéal premier : c'est l'idéal engendré par $X + 1$. En remontant les isomorphismes, on déduit que l'unique idéal de A contenant 2 est l'idéal $(1 + i\sqrt{11}, 2)$.

Si (2) était produit d'idéaux premiers dans A, il existerait $n \geq 1$ tel que :

$$(2) = (1 + i\sqrt{11}, 2)^n.$$

Or on remarque que :

$$(1 + i\sqrt{11}, 2)^2 = (4, 2 + 2i\sqrt{11})$$

ne contient pas 2 et donc que :

$$(1 + i\sqrt{11}, 2)^2 \subsetneq (2) \subsetneq (1 + i\sqrt{11}, 2).$$

Cela montre que (2) n'est pas produit d'idéaux premiers dans A.

Remarque : Ce phénomène vient du fait que A n'est pas l'anneau des entiers de A. En fait l'anneau des entiers de A est $\mathbb{Z}[\frac{1+i\sqrt{11}}{2}]$.

3. À l'inverse, montrer que les idéaux (2), (3) et (7) s'écrivent bien comme des produit d'idéaux premiers de l'anneau B.

Indications : On a :

$$B/(2) \cong \mathbb{Z}/2\mathbb{Z}[X]/(X+1)^2$$
$$B/(3) \cong \mathbb{Z}/3\mathbb{Z}[X]/(X^2+1)$$
$$B/(7) \cong \mathbb{Z}/7\mathbb{Z}[X]/((X+1)(X-1)).$$

Ainsi $\mathfrak{p}_2 = (2, 1+i\sqrt{13})$ est l'unique idéal de B contenant 2, l'idéal $\mathfrak{p}_3 = (3)$ est premier dans B (et c'est le seul idéal premier de B contenant (3)) et $\mathfrak{p}_7 = (7, 1+i\sqrt{13})$ et $\mathfrak{p}_7' = (7, 1-i\sqrt{13})$ sont les idéaux de B contenant (7). On vérifie alors aisément que :

$$(2) = \mathfrak{p}_2^2, \qquad (3) = \mathfrak{p}_3 \qquad (7) = \mathfrak{p}_7\mathfrak{p}_7'.$$

Remarque : L'anneau B est l'anneau des entiers de $\mathbb{Q}(i\sqrt{13})$. C'est un anneau de Dedekind, donc tout idéal est produit d'idéaux premiers. En fait, si p est un nombre premier, il est intéressant de comprendre comment l'idéal (p) de B se décompose en produit d'idéaux premiers. Dans ce cas, seuls 3 comportements sont possibles : ce sont ceux que nous avons observés en répondant à la question pour $p = 2, 3, 7$. On dit que le cas $p = 2$ est ramifié, alors que les cas $p = 3$ et $p = 7$ sont non ramifiés. Dans le cas de $p = 7$, on dit en plus que (7) est totalement décomposé dans B.

Exercice 5 : Anneau de polynômes

Soit A un anneau commutatif unitaire. Montrer que si A n'est pas un corps, alors $A[X]$ n'est pas principal.

Indications : Supposons A intègre (dans le cas contraire, $A[X]$ ne l'est pas non plus et n'est donc pas principal). Soit $a \in A \setminus (A^\times \cup \{0\})$. Montrons que l'idéal $I = (a)+(X)$ n'est pas principal. En effet, supposons $I = (b)$ avec $b \in A[X]$. Alors, comme on a $\deg(\alpha\beta) = \deg(\alpha)+\deg(\beta)$, on a nécessairement $\deg(b) \leq \deg(a) = 0$, c'est-à-dire $b \in A$. De plus, il existe $c \in A[X]$ vérifiant $bc = X$. On a alors $\deg(c) = 1$, et donc il existe $d, e \in A$ tels que $dX + e = c$. Mais on a ainsi $bd = 1$. Cela implique $I = A[X]$, ce qui est absurde puisque son image par la projection $A[X] \twoheadrightarrow A$ est $(a) \neq A$.

Exercice 6 : Exemples d'anneaux non factoriels

1. Montrer que l'anneau $A = \mathbb{C}[X, Y, Z, T]/(XY - ZT)$ est intègre mais pas factoriel.

Indications : Considérons le morphisme :

$$\varphi : \mathbb{C}[X,Y,Z,T] \to \mathbb{C}(Z)[X,Y], X \mapsto X, Y \mapsto Y, Z \mapsto Z, T \mapsto \frac{XY}{Z}.$$

On vérifie aisément que $(XY - ZT) \subseteq \text{Ker } \varphi$. Montrons qu'il y a égalité.
Soit $P \in \text{Ker } \varphi$. Comme on a $X^aY^bZ^cT^d = X^{a+c}Y^{b+c}T^{d-c}$ ou $X^aY^bZ^cT^d = X^{a+d}Y^{b+d}T^{c-d}$ dans A, il existe des polynômes $Q(X,Y) \in \mathbb{C}[X,Y]$, $R(X,Y,Z) \in \mathbb{C}[X,Y,Z]$ et $S(X,Y,T) \in \mathbb{C}[X,Y,T]$ tels que $P \equiv Q(X,Y) + ZR(X,Y,Z) + TS(X,Y,T) \mod XY - ZT$. On a alors $0 = \varphi(P) = Q(X,Y) + ZR(X,Y,Z) + \frac{XY}{Z}S(X,Y,\frac{XY}{Z})$, ce qui montre que $Q = R = S = 0$. Par conséquent, $P \in (XY - ZT)$ et $\text{Ker } \varphi = (XY - ZT)$. Le morphisme φ induit donc un morphisme injectif $A \to \mathbb{C}(Z)[X,Y]$, ce qui montre que A est intègre.
Montrons que A n'est pas factoriel. Dans A, on a la relation $XY = ZT$. Il suffit donc de montrer que X, Y, Z, T sont irréductibles dans A. Par symétrie des rôles, il suffit de montrer l'irréductibilité de X. On remarque déjà que X n'est pas inversible puisque son image par φ ne l'est pas. Soient maintenant P_1 et P_2 dans $\mathbb{C}[X,Y,Z,T]$ tels que $X \equiv P_1P_2 \mod XY - ZT$. On a alors $X = \varphi(P_1)\varphi(P_2)$. Comme X est irréductible dans $\mathbb{C}(Z)[X,Y]$, il existe $F(Z) \in \mathbb{C}(Z)$ non nul tel que $\varphi(P_1) = F$ ou $\varphi(P_2) = F$. Supposons sans perte de généralité que $\varphi(P_1) = F$. Comme précédemment, on peut trouver :

- $Q_1(X,Y) \in \mathbb{C}[X,Y]$, $R_1(X,Y,Z) \in \mathbb{C}[X,Y,Z]$ et $S_1(X,Y,T) \in \mathbb{C}[X,Y,T]$ tels que $P_1 \equiv Q_1(X,Y) + ZR_1(X,Y,Z) + TS_1(X,Y,T) \mod XY - ZT$;
- $Q_2(X,Y) \in \mathbb{C}[X,Y]$, $R_2(X,Y,Z) \in \mathbb{C}[X,Y,Z]$ et $S_2(X,Y,T) \in \mathbb{C}[X,Y,T]$ tels que $P_2 \equiv Q_2(X,Y) + ZR_2(X,Y,Z) + TS_2(X,Y,T) \mod XY - ZT$.

On a alors $Q_1(X,Y) + ZR_1(X,Y,Z) + \frac{XY}{Z}S_1(X,Y,\frac{XY}{Z}) = F(Z)$. Cela montre que $S_1 = 0$, $Q_1 \in \mathbb{C}$ et $R_1 \in \mathbb{C}[Z]$. En notant :

$$\psi : A \to \mathbb{C}(X)[Z,T], X \mapsto X, Y \mapsto \frac{ZT}{X}, Z \mapsto Z, T \mapsto T,$$

on remarque que $\psi(Z)$ ne divise pas $\psi(X)$. Donc Z ne divise pas X dans A et $Q_1 \neq 0$.
Par ailleurs, on a $\varphi(P_2) = \frac{X}{Q_1 + ZR_1(Z)} = Q_2(X,Y) + ZR_2(X,Y,Z) + \frac{XY}{Z}S_2(X,Y,\frac{XY}{Z})$. Comme $Q_1 \in \mathbb{C}^\times$, on en déduit que $R_1 = 0$ et donc P_1 est inversible dans A. Cela montre que X est irréductible dans A.

2. Montrer que l'anneau $B = \mathbb{Z}[\sqrt{10}]$ n'est pas factoriel, mais que tout élément non nul de B s'écrit sous la forme $up_1...p_n$ avec $u \in B^\times$ et p_i irréductible pour chaque i.

Indications : Dans B, on a la relation $2 \times 5 = (\sqrt{10})^2$. Montrons que 2 est irréductible dans B. Écrivons donc $2 = yz$ et notons $N : B \to \mathbb{N}, a + b\sqrt{10} \mapsto |a^2 - 10b^2|$. On remarque alors que $4 = N(2) = N(yz) = N(y)N(z)$. Si $N(y) = N(z) = 2$, alors il existerait $a, b \in \mathbb{Z}$ tels que $|a^2 - 10b^2| = 2$: absurde (regarder modulo 5). Par conséquent, $N(y) = 1$ ou $N(z) = 1$, et alors y ou z est une unité. Donc 2 est irréductible dans B. Comme 2 ne divise pas $\sqrt{10}$, B n'est pas factoriel. Montrons que tout élément x de B s'écrit sous la forme $up_1...p_n$ avec $u \in B^\times$ et p_i irréductible pour chaque i. On procède par récurrence sur $N(x)$. Si $N(x) = 1$, alors x est un unité et la propriété est vraie. Supposons que la propriété soit vraie pour x tel que $N(x) \leq n$. Soit $x \in B$ tel que $N(x) = n + 1$. Si x est irréductible, alors on a terminé. Sinon, il existe y et z dans $B \setminus B^\times$ tels que $x = yz$. On a alors $N(y) < n+1$ et $N(z) < n+1$. On peut donc appliquer l'hypothèse de récurrence à y et z, et on obtient une écriture de x sous la forme $up_1...p_n$ avec $u \in B^\times$ et p_i irréductible pour chaque i.

3. Plus généralement, est-il vrai que, si p et q sont deux nombres premiers distincts, alors l'anneau $\mathbb{Z}[\sqrt{pq}]$ n'est pas factoriel ?

Indications : Non. Prenons $p = 2$ et $q = 3$, et considérons $C = \mathbb{Z}[\sqrt{6}]$. Montrons que C est un anneau euclidien. Notons $N : \mathbb{Q}[\sqrt{6}] \to \mathbb{N}, a_1 + a_2\sqrt{6} \mapsto |a_1^2 - 6a_2^2|$. Soient $x, y \in C$ avec $x \neq 0$ et $y \neq 0$. On écrit $\frac{x}{y} = c_1 + c_2\sqrt{6}$ avec $c_1, c_2 \in \mathbb{Q}$, et on note d_1 (resp. d_2) des entiers tels que $|d_1 - c_1| \leq 1/2$ et $|d_2 - c_2| \leq 1/2$. Plusieurs cas se présentent :

- si $6(d_2 - c_2)^2 < 1$, alors on a $N(\frac{x}{y} - (d_1 + d_2\sqrt{6})) < 1$;
- si $1 \leq 6(d_2 - c_2)^2 < \frac{5}{4}$, alors $N(\frac{x}{y} - (1 + d_1 + d_2\sqrt{6})) < 1$;
- si $\frac{5}{4} \leq 6(d_2 - c_2)^2 < \frac{3}{2}$, alors $N(\frac{x}{y} - (-1 + d_1 + d_2\sqrt{6})) < 1$.

Dans tous les cas, on trouve $q \in C$ tel que $N(\frac{x}{y} - q) < 1$. Par conséquent, en posant $r = x - qy$, on a $x = qy + r$ avec $N(r) = N(\frac{x}{y} - q)N(y) < N(y)$. Donc C est euclidien.

Remarque : L'égalité $2 \times 3 = (\sqrt{6})^2$ n'implique pas que C n'est pas factoriel, parce que 2, 3 et $\sqrt{6}$ ne sont pas irréductibles : on a $2 = (\sqrt{6} + 2)(\sqrt{6} - 2)$, $3 = (3 + \sqrt{6})(3 - \sqrt{6})$ et $\sqrt{6} = (\sqrt{6} + 2)(3 - \sqrt{6}) = (\sqrt{6} - 2)(3 + \sqrt{6})$.

Exercice 7 : Un anneau principal non euclidien

Soit R un anneau euclidien qui n'est pas un corps.

1. Montrer que l'on peut trouver un élément non inversible x de R tel que la restriction à $R^\times \cup \{0\}$ de la projection canonique de R sur $R/(x)$ soit surjective. On pourra choisir x tel que $\phi(x)$ soit minimal parmi les éléments $x \notin R^\times$, où ϕ désigne le stathme d'une division euclidienne de R.

Indications : Soit $x \in R \setminus (R^\times \cup \{0\})$ tel que $\phi(x)$ est minimal. Soit $\overline{y} \in R/(x)$. Soit $y \in R$ un relèvement de $\overline{y}$. On écrit la division euclidienne de y par x : on trouve ainsi $q, r \in R$ tels que $y = qx + r$, $\phi(r) < \phi(x)$ et $r \neq 0$. Par définition de x, on a $r \in R^\times \cup \{0\}$, et r est un relèvement de $\overline{y}$ dans R, ce qui achève la preuve.

Soient $\alpha = \frac{1+i\sqrt{19}}{2}$ et $A = \mathbb{Z}[\alpha]$.

2. Déterminer $A^\times$.

Indications : On définit $N : \mathbb{Q}[\alpha] \to \mathbb{N}, z \mapsto |z|^2$. On vérifie immédiatement que :

$$\forall z \in A, z \in A^\times \Leftrightarrow N(z) = 0.$$

Comme $N(a + b\frac{1+i\sqrt{19}}{2}) = (a + \frac{b}{2})^2 + \frac{19}{4}b^2$, on vérifie alors que $A^\times = \{-1, 1\}$.

3. Montrer que A n'est pas euclidien.

Indications : Supposons A euclidien. Alors il existe $x \in A \setminus A^\times$ tel que la projection $A^\times \cup \{0\} \to A/(x)$ est surjective. On en déduit que $A/(x)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ ou à $\mathbb{Z}/3\mathbb{Z}$. Mais le polynôme $X^2 - X + 5$, qui annule α, ne possède pas de racines dans $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$: absurde !

4. Si $a, b \in A \setminus \{0\}$, montrer qu'il existe $q, r \in A$ tels que $r = 0$ ou $|r| < |b|$ et qui vérifient, soit $a = bq + r$, soit $2a = bq + r$.

Indications : On écrit $ab^{-1} = u + v\alpha \in \mathbb{Q}[\alpha]$, et on note $n = \lfloor v \rceil$.
Supposons $v \notin]n + \frac{1}{3}, n + \frac{2}{3}[$ et soient $s, t \in \mathbb{Z}$ les entiers les plus proches de u et v respectivement. Par hypothèse sur v, on a $|t - v| \leq \frac{1}{3}$ et $|s - u| \leq \frac{1}{2}$. On pose alors $q = s + t\alpha \in A$, et on a

$$N(ab^{-1} - q) = (u - s)^2 + (u - s)(v - t) + 5(v - t)^2 < 1.$$

Dans le cas où v appartient à $]n + \frac{1}{3}, n + \frac{2}{3}[$, on considère $2ab^{-1}$, qui nous ramène au cas précédent.

5. Montrer que $A/(2)$ est un corps. On pourra utiliser l'exercice 5.

Indications : On utilise $A \simeq \mathbb{Z}[T]/(T^2 - T + 5)$ pour écrire :

$$A/2A \cong \mathbb{Z}/2\mathbb{Z}[T]/(T^2 + T + 1).$$

Comme $T^2 + T + 1$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[T]$, on déduit que $A/(2)$ est un corps.

6. Montrer que A est un anneau principal.

Indications : Soient I un idéal non nul et b un élément non nul de I avec $N(b)$ minimal. Soit $a \in I$. En utilisant 4., on a q, r vérifiant $a = bq + r$ ou $2a = bq + r$. Dans le premier cas, on a $r = 0$ par minimalité de $N(b)$ et c'est gagné. Dans le second cas, on a de même $r = 0$ et donc $2a = bq$. Comme $2A$ est maximal, on a $b \in 2A$ ou $q \in 2A$. Dans ce dernier cas, on conclut directement. Il reste donc à examiner le cas $q \notin 2A$ et $b = 2c$ avec $c \in A$. Par 5., on a alors $2A + qA = A$, et il existe alors $x, y \in A$ tels que $c = c \cdot 1 = 2xc + qyc = bx + ay \in I$. Ceci contredit alors la minimalité de b, et ce cas de figure n'est pas envisageable.

Exercice 8 : Une équation diophantienne

1. Montrer que $\mathbb{Z}[\frac{1+i\sqrt{11}}{2}]$ est un anneau euclidien. Quelles sont ses unités ?

2. Trouver tous les couples $(x, y) \in \mathbb{Z}^2$ tels que $y^2 + 11 = x^3$.

Exercice 9 : Autres équations diophantiennes

Attention : J'ai fait les calculs de cet exercice assez rapidement... Il se peut que j'aie fait des erreurs de calcul !

1. Trouver tous les couples d'entiers (x, y) tels que $y^2 + 2 = x^3$.

Indications : On pose $A = \mathbb{Z}[i\sqrt{2}]$, puis on montre que A est euclidien pour le stathme $N : A \to \mathbb{N}, z \mapsto |z|^2$ et que $A^\times = \{1, -1\}$. On vérifie que y n'est pas multiple de 2, et on en déduit que $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux dans A. En écrivant que $y + i\sqrt{2}$ est un cube, on arrive alors aux solutions $(x, y) = (3, \pm 5)$.

2. Trouver tous les couples d'entiers (x, y) tels que $y^2 + 11 = 4x^5$.

Indications : On pose $A = \mathbb{Z}[\frac{1+i\sqrt{11}}{2}]$, puis on montre que A est euclidien pour le stathme $N : A \to \mathbb{N}, z \mapsto |z|^2$ et que $A^\times = \{1, -1\}$. On vérifie que y n'est pas multiple de 11, et on en déduit que y est impair et que $(y+i\sqrt{11}) \wedge (y-i\sqrt{11}) = 2$. En écrivant que $\frac{y+i\sqrt{11}}{2}$ est une puissance cinquième, on arrive aux solutions $(x, y) = (3, \pm 31)$.

3. Trouver tous les couples d'entiers (x, y) tels que $y^2 + y + 2 = x^5$.

Indications : L'équation se réécrit $(2y + 1)^2 + 7 = 4x^5$. On pose $A = \mathbb{Z}[\frac{1+i\sqrt{7}}{2}]$, puis on montre que A est euclidien pour le stathme $N : A \to \mathbb{N}, z \mapsto |z|^2$ et que $A^\times = \{1, -1\}$. On vérifie que $2y + 1$ n'est pas multiple de 7, et on en déduit que $(2y + 1 + i\sqrt{7}) \wedge (2y + 1 - i\sqrt{7}) = 2$. En écrivant que $\frac{2y+1+i\sqrt{7}}{2}$ est une puissance cinquième, on arrive aux solutions $(x, y) = (2, 5)$ et $(x, y) = (2, -6)$.

4. Trouver tous les couples d'entiers impairs (x, y) tels que $y^2 + 28 = x^3$.

Indications : On pose $A = \mathbb{Z}[\frac{1+i\sqrt{7}}{2}]$, puis on montre que A est euclidien pour le stathme $N : A \to \mathbb{N}, z \mapsto |z|^2$ et que $A^\times = \{1, -1\}$. On vérifie que y n'est pas multiple de 7, et on en déduit que $y + 2i\sqrt{7}$ et $y - 2i\sqrt{7}$ sont premiers entre eux dans A. En écrivant que $y + 2i\sqrt{7}$ est un cube, on arrive alors aux solutions $(x, y) = (37, \pm 225)$.

Exercice 10 : Sommes de deux carrés

On cherche à déterminer $S = \{a^2 + b^2 | (a, b) \in \mathbb{Z}^2\}$.

1. (a) Quels sont les nombres premiers p tels que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$?

(b) En déduire que, si p est un nombre premier congru à 3 modulo 4 et n un élément non nul de S, alors $v_p(n)$ est pair.

2. Rappeler pourquoi l'anneau $\mathbb{Z}[i]$ est principal. Quelles sont ses unités ?

3. (a) Montrer qu'un nombre premier p est dans S si, et seulement si, il n'est pas irréductible dans $\mathbb{Z}[i]$.

(b) En déduire qu'un nombre premier impair p est dans S si, et seulement si, il est congru à 1 modulo 4. On pourra utiliser le résultat de l'exercice 5.

4. Montrer qu'un entier naturel n est dans S si, et seulement si, pour tout premier p congru à 3 modulo 4, la valuation $v_p(n)$ est paire.

Exercice 11 : Entiers de la forme $a^2 + ab + b^2$

S'inspirer de l'exercice précédent pour déterminer l'ensemble $T = \{a^2 + ab + b^2 \mid (a, b) \in \mathbb{Z}^2\}$.

Indications : On note $\rho = e^{2i\pi/3}$. On procède exactement de la même manière que dans l'exercice précédent, en remplaçant A par l'anneau principal $B = \mathbb{Z}[\rho]$. On montre que B est euclidien pour $N : a + b\rho \mapsto a^2 - ab + b^2$, et on montre qu'un nombre premier est dans T si, et seulement si, il n'est pas irréductible dans B si, et seulement si, il est congru à 0 ou 1 modulo 3. On déduit que les T est formé des entiers naturels dont la valuation p-adique est paire pour tout premier p congru à 2 modulo 3.

Exercice 12 : Les entiers de la forme $a^2 - 2b^2$

On cherche à déterminer $S = \{a^2 - 2b^2 \mid (a, b) \in \mathbb{Z}^2\}$. Pour ce faire, on pose $A = \mathbb{Z}[\sqrt{2}]$.

1. Dans cette question, nous allons déterminer les nombres premiers p tels que 2 est un carré modulo p.

(a) On suppose que $p \equiv 1 \mod 8$. Montrer que -1 est une puissance quatrième dans $\mathbb{Z}/p\mathbb{Z}$. En déduire que 2 est bien un carré modulo p.

Indications : On a $(\mathbb{Z}/p\mathbb{Z})^\times \equiv \mathbb{Z}/(p-1)\mathbb{Z}$. Comme $8|p-1$, on en déduit que ce groupe possède un élément z d'ordre 8 : c'est une racine quatrième de -1 dans $\mathbb{Z}/p\mathbb{Z}$. On a donc $z^4 = -1$ dans $\mathbb{Z}/p\mathbb{Z}$, d'où $(z + z^{-1})^2 = 2$.

Dans la suite de cette question, on supposera que p est impair.

(b) Soit $P \in \mathbb{Z}/p\mathbb{Z}[X]$ un polynôme irréductible divisant $X^4 + 1$. Montrer que l'anneau $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ est un corps contenant $\mathbb{Z}/p\mathbb{Z}$ comme sous-corps et possédant une racine quatrième de -1. On notera $k = \mathbb{Z}/p\mathbb{Z}[X]/(P)$ et α une racine quatrième de -1 dans k.

Indications : Comme P est irréductible et $\mathbb{Z}/p\mathbb{Z}[X]$ est un anneau principal, $\mathbb{Z}/p\mathbb{Z}[X]/(P)$ est un corps. Il contient évidemment $\mathbb{Z}/p\mathbb{Z}$ comme sous-corps et la classe de X est une racine quatrièment de -1 dans $\mathbb{Z}/p\mathbb{Z}[X]/(P)$.

(c) Vérifier que les éléments x de k vérifiant $x^2 = 2$ sont $\alpha + \alpha^{-1}$ et $-\alpha - \alpha^{-1}$.

Indications : On a $\alpha^4 = 1$, donc $(\alpha + \alpha^{-1})^2 = \alpha^2 + \alpha^{-2} + 2 = 2$. On en déduit que $\alpha + \alpha^{-1}$ et $-\alpha - \alpha^{-1}$ sont des racines carrées de 2 dans k. Comme k est un corps, ce sont les seules.

(d) Montrer qu'un élément x de k est dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $x^p = x$.

Indications : Si $x \in \mathbb{Z}/p\mathbb{Z}$, alors $x^p = x$ car $(\mathbb{Z}/p\mathbb{Z})^\times$ est d'ordre $p-1$. Comme le polynôme $X^p - X$ est de degré p, il possède au plus p racines. On en déduit qu'un élément x de k est dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $x^p = x$.

(e) Déduire des deux questions précédentes que 2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, p est congru à 1 ou 7 modulo 8.

Indications : Si p est congru à 1 ou à 7 modulo 8, on a $(\alpha+\alpha^{-1})^p = \alpha^p+\alpha^{-p} = \alpha + \alpha^{-1}$, et donc $\alpha + \alpha^{-1} \in \mathbb{Z}/p\mathbb{Z}$. On en déduit que 2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$. Si p est congru à 3 ou 5 modulo 8, on a $(\alpha + \alpha^{-1})^p = \alpha^p + \alpha^{-p} = -\alpha - \alpha^{-1}$, et donc $\alpha + \alpha^{-1} \notin \mathbb{Z}/p\mathbb{Z}$. Donc 2 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$

2. Montrer que l'anneau A est euclidien.

> **Indications :** Soit $N : A \to \mathbb{N}, a+b\sqrt{2} \mapsto |a^2-2b^2|$. Soient $x, y \in A$ avec $x \neq 0$ et $y \neq 0$. On écrit $\frac{x}{y} = c_1 + c_2\sqrt{2}$ avec $c_1, c_2 \in \mathbb{Q}$, et on note d_1 (resp. d_2) des entiers tels que $|d_1 - c_1| \leq 1/2$ et $|d_2 - c_2| \leq 1/2$. Alors $N(\frac{x}{y} - (d_1 + d_2\sqrt{2})) \leq \frac{3}{4} < 1$. On trouve donc $q \in A$ tel que $N(\frac{x}{y} - q) < 1$. Par conséquent, en posant $r = x - qy$, on a $x = qy + r$ avec $N(r) = N(\frac{x}{y} - q)N(y) < N(y)$. Donc A est euclidien.

3. Soit n un entier. Montrer que, si $n \in S$, alors $-n \in S$.

> **Indications :** Soit $N' : A \to \mathbb{N}, a+b\sqrt{2} \mapsto a^2-2b^2$. Supposons que $n \in S$. Soient $a, b \in \mathbb{Z}$ tels que $N'(a+b\sqrt{2}) = n$. On remarque alors que $N'((1+\sqrt{2})(a+b\sqrt{2})) = N'(1+\sqrt{2})N'(a+b\sqrt{2}) = -n$. Donc $-n \in S$.

4. Quels sont les nombres premiers impairs p qui sont irréductibles dans A ?

> **Indications :** Comme A est principal, un nombre premier p est irréductible dans A ssi $A/(p)$ est intègre. Or $A/(p) \cong \mathbb{Z}/p\mathbb{Z}[X]/(X^2-2)$. Cet anneau est intègre si, et seulement si, 2 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire si, et seulement si, p est congru à 3 ou à 5 modulo 8.

5. En déduire qu'un nombre premier impair p est dans S si, et seulement si, il est congru à 1 ou 7 modulo 8.

> **Indications :** Si p est congru 1 ou 7 modulo 8, alors p n'est pas irréductible dans A : on écrit $p = xy$ avec $x, y \in \mathbb{Z}[\sqrt{2}]$ tels que $N(x) \neq 1$ et $N(y) \neq 1$. On a alors $N(x) = N(y) = p$, et donc $p \in S$. Réciproquement, si $p \in S$, on écrit $p = a^2 - 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2})$. On en déduit que p n'est pas irréductible dans A et donc que p est congru à 1 ou 7 modulo 8.

6. Caractériser S.

> **Indications :** L'ensemble S est constitué des entiers (relatifs) tels que, pour tout premier p congru à 3 ou 5 modulo 8, la valuation p-adique de n est paire. La preuve est tout à fait analogue aux questions 1.b) et 4. de l'exercice 13.

7. Soit $n \in S$. Montrer qu'il existe une infinité de couples $(a, b) \in \mathbb{Z}^2$ tels que $n = a^2 - 2b^2$.

> **Indications :** Soit $z \in A$ tel que $N'(z) = n$. On remarque alors que, pour tout entier m, on a $N'((3 + 2\sqrt{2})^m z) = N'(3 + 2\sqrt{2})^m N'(z) = N'(z) = n$. Il existe donc une infinité de couples $(a, b) \in \mathbb{Z}^2$ tels que $n = a^2 - 2b^2$.