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

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.
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.

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.

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.

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.

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.

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 ?

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.

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

2. Déterminer $A^\times$.

3. Montrer que A n'est pas euclidien.

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 $2a = bq + r$.

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

6. Montrer que A est un anneau principal.

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

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

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

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

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

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 $T = \{a^2 + ab + b^2 \mid (a, b) \in \mathbb{Z}^2\}$.

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.

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.

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

(d) Montrer 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.

2. Montrer que l'anneau A est euclidien.

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

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

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.

6. Caractériser S.

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