USTC - Feuille de TD 2

Diego Izquierdo

1 Divisibilité dans les anneaux

Exercice 1 Soit $A = \mathbb{Z}[\sqrt{5}]$.

1) Montrer que A possède une infinité d'éléments inversibles.
2) Montrer que 2, $3+\sqrt{5}$ et $3-\sqrt{5}$ sont irréductibles dans A.
3) Montrer qu'il n'y a pas d'unicité de la décomposition de 4 en facteurs irréductibles dans A.
4) Vérifier que 2 et $3+\sqrt{5}$ sont associés dans $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. De même, vérifier que 2 et $3-\sqrt{5}$ sont associés dans $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Remarque : On verra dans l'exercice 25 que tout élément non nul de $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ s'écrit comme produit d'irréductibles, et ce de manière unique à l'ordre et à une unité près.

Exercice 2 Soit $A = \mathbb{Z}[i\sqrt{5}]$.

1) Quels sont les éléments inversibles de A ?
2) Montrer que 3, 7, $4-i\sqrt{5}$ et $4+i\sqrt{5}$ sont irréductibles dans A.
3) Montrer qu'il n'y a pas d'unicité de la décomposition de 21 en facteurs irréductibles dans A.
4) Considérons les idéaux :

$$\mathfrak{p}_1 = (3, i\sqrt{5}-1), \quad \mathfrak{p}_2 = (3, i\sqrt{5}+1),$$

$$\mathfrak{q}_1 = (7, i\sqrt{5}+3), \quad \mathfrak{q}_2 = (7, i\sqrt{5}-3).$$

Vérifier que ce sont des idéaux premiers et que :

$$(3) = \mathfrak{p}_1\mathfrak{p}_2, \quad (7) = \mathfrak{q}_1\mathfrak{q}_2, \quad (4+i\sqrt{5}) = \mathfrak{p}_2\mathfrak{q}_2, \quad (4-i\sqrt{5}) = \mathfrak{p}_1\mathfrak{q}_1.$$

Remarque : On peut montrer que, dans l'anneau A, tout idéal s'écrit comme produit d'idéaux premiers, et ce de manière unique à l'ordre près.

Exercice 3 Soit A un anneau commutatif.

1) Supposons A intègre. Rappeler pourquoi, si a et b sont deux éléments de A tels que $(a) = (b)$, alors il existe $u \in A^\times$ tel que $a = bu$.

Prenons maintenant $A = \mathbb{Q}[X, Y, Z]/(X - XYZ)$. On note x, y et z les classes de X, Y et Z dans A.

1) Vérifier que A n'est pas intègre.
2) Montrer que $(x) = (xy)$.
3) Montrer qu'il n'existe pas d'élément $u \in A^\times$ tel que $xu = xy$.

2 Anneaux euclidiens et principaux

Exercice 4 Montrer que l'anneau des nombres décimaux (c'est-à-dire les nombres rationnels dont le développement décimal est fini) est principal. Quel est le pgcd de $0,6$ et de $30,4$?

Exercice 5 Soit A un anneau commutatif. Montrer que si A n'est pas un corps, alors $A[X]$ n'est pas principal.

Exercice 6 Soit $\mathcal{C}$ (resp. $\mathcal{C}^\infty$) l'anneau des fonctions continues (resp. C^∞) de $[0,1]$ dans $\mathbb{R}$.

1) Montrer que les idéaux maximaux de $\mathcal{C}$ sont les

$$I_x = \{f \in \mathcal{C} \mid f(x) = 0\}$$

pour $x \in [0,1]$. Sont-ils principaux ?

2) Montrer que les idéaux maximaux de $\mathcal{C}^\infty$ sont les $I_x \cap \mathcal{C}^\infty$. Sont-ils principaux ?

Exercice 7

1) Trouver tous les couples $(x,y) \in \mathbb{Z}^2$ tels que $y^2 = x^3 + 16$.
2) Trouver tous les couples $(x,y) \in \mathbb{C}[T]^2$ tels que $y^2 + T = x^3$.

Exercice 8 Dans cet exercice, on étudie l'anneau des entiers de Gauss $\mathbb{Z}[i]$.

1) Rappeler pourquoi l'anneau $\mathbb{Z}[i]$ est principal. Quelles sont ses unités ?
2) Soit p un nombre premier impair. Montrer que les assertions suivantes sont équivalentes :
   i) p n'est pas irréductible dans $\mathbb{Z}[i]$.
   ii) Il existe $(a,b) \in \mathbb{Z}^2$ tel que $p = a^2 + b^2$.
   iii) -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
   iv) p est congru à 1 modulo 4.
3) L'élément 2 est-il irréductible dans $\mathbb{Z}[i]$?
4) a) Montrer que tout irréductible de $\mathbb{Z}[i]$ divise un unique nombre premier de $\mathbb{Z}$.
   b) En déduire la liste des éléments irréductibles de $\mathbb{Z}[i]$

Exercice 9 Déduire de l'exercice précédent qu'un entier naturel n est somme de deux carrés si, et seulement si, pour tout premier p congru à 3 modulo 4, la valuation $v_p(n)$ est paire.

Exercice 10 Factoriser $-3 + 15i$ en irréductibles dans $\mathbb{Z}[i]$.

Exercice 11 En utilisant l'exercice 8, trouver toutes les seules solutions entières de l'équation $y^2 + 4 = x^3$.

Exercice 12 Dans cet exercice, on étudie l'anneau des entiers d'Eisenstein $\mathbb{Z}[j]$, avec $j = e^{2i\pi/3}$.

1) Montrer que l'anneau $\mathbb{Z}[j]$ est principal. Quelles sont ses unités ?
2) Soit p un nombre premier différent de 3. Montrer que les assertions suivantes sont équivalentes :
   i) p n'est pas irréductible dans $\mathbb{Z}[i]$.
   ii) Il existe $(a, b) \in \mathbb{Z}^2$ tel que $p = a^2 - ab + b^2$.
   iii) Le polynôme $X^3 - 1$ a une racine dans $\mathbb{Z}/p\mathbb{Z}$ autre que 1.
   iv) p est congru à 1 modulo 3.
3) L'élément 3 est-il irréductible dans $\mathbb{Z}[j]$?
4) a) Montrer que tout irréductible de $\mathbb{Z}[j]$ divise un unique nombre premier de $\mathbb{Z}$.
   b) En déduire la liste des éléments irréductibles de $\mathbb{Z}[j]$

Exercice 13 Utiliser l'exercice précédent pour déterminer quels entiers naturels n s'écrivent sous la forme $a^2 - ab + b^2$ avec $a, b \in \mathbb{Z}$.

Exercice 14 Factoriser $9 + 3j + 6j^2$ en irréductibles dans $\mathbb{Z}[j]$.

Exercice 15 [Théorème de Fermat pour $n = 3$] Supposons qu'il existe des éléments non nuls x, y, z dans A tels que

$$x^3 + y^3 = z^3,$$

et posons $A = \mathbb{Z}[j]$. On note $N : w \mapsto w\overline{w}$ la norme usuelle. On pourra utiliser librement l'exercice 12.

1) Montrer que l'on peut supposer x, y, z premiers entre eux, ce que l'on suppose dans la suite.
2) Montrer que tout élément de A est congru à $0, 1$ ou -1 modulo $\theta := i\sqrt{3}$.
3) Soit ξ et η dans A non divisibles par θ. Montrer que

$$\begin{aligned}
\xi \equiv 1 \mod \theta &\implies \xi^3 \equiv 1 \mod 9 \\
\xi \equiv -1 \mod \theta &\implies \xi^3 \equiv -1 \mod 9 \\
\xi^3 + \eta^3 \equiv 0 \mod \theta &\implies \xi^3 + \eta^3 \equiv 0 \mod 9 \\
\xi^3 - \eta^3 \equiv 0 \mod \theta &\implies \xi^3 + \eta^3 \equiv 0 \mod 9
\end{aligned}$$

4) Montrer que θ divise et et un seul des entiers x, y, z.
5) On suppose qu'il existe x, y, z dans A tels que θ ne divise pas xyz, des unités $\varepsilon_1, \varepsilon_2$ et un entier $r > 0$ tels que

$$x^3 + \varepsilon_1 y^3 + \varepsilon_2 (\theta^r z)^3 = 0.$$

   Montrer que $\varepsilon_1 = \pm 1$ et $r \geqslant 2$.
6) Considérons x, y, z non nuls dans A vérifiant $x^3 + y^3 + \varepsilon(\theta^r z)^3 = 0$, avec $r \geqslant 2$, ε une unité de A et θ ne divisant pas xyz. Supposons que $N(x^3 y^3 z^3 \theta^{3r})$ soit minimale dans $\mathbb{Z}$. Obtenir une contradiction en construisant un autre triplet (x', y', z') de norme strictement plus petite et conclure.

Exercice 16 On considère l'anneau $A = \mathbb{Z}[i\sqrt{2}]$. Montrer que A est un anneau euclidien et en déduire les solutions entières de l'équation $y^2 + 2 = x^3$.

Exercice 17 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 $\alpha = \dfrac{1+i\sqrt{19}}{2}$ et $A = \mathbb{Z}[\alpha]$.

2) Déterminer $A^\times$.
3) Montrer que A n'est pas euclidien.
4) Si $a, b \in A \smallsetminus \{0\}$, 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 l'idéal engendré par 2 dans A est maximal.
6) Montrer que A est un anneau principal.

Exercice 18 Soit A un anneau intègre dans lequel tout idéal premier est principal. Montrer que l'anneau A est principal (*Indication :* on pourra considérer un élément maximal I dans la famille des idéaux non principaux de A, des éléments x et y de $A \smallsetminus I$ tels que $xy \in I$, un générateur z de l'idéal $I + (x)$, un générateur w de l'idéal $\{a \in A \mid az \in I\}$, et montrer que zw engendre I).

Exercice 19 Trouver toutes les solutions entières de l'équation $999x - 49y = 5000$, puis celles de l'équation $147x + 258y = 369$.

Exercice 20 Soit $P = X^3 + 1$ et $Q = X^2 + 1$. Montrer que P et Q sont premiers entre eux dans $\mathbb{Q}[X]$ et trouver $U, V \in \mathbb{Q}[X]$ tels que $UP + VQ = 1$.

Exercice 21 Résoudre les systèmes :

$$\begin{cases} x \equiv 2 \mod 25 \\ x \equiv 3 \mod 8 \\ x \equiv 1 \mod 3. \end{cases} \quad , \quad \begin{cases} P \equiv X \mod X^3 - X + 1 \\ P \equiv X^2 + 1 \mod X^4. \end{cases}$$

3 Anneaux factoriels

Exercice 22 Chercher un exemple d'anneau factoriel non principal et deux éléments a et b de cet anneau tel que l'inclusion d'idéaux $(a, b) \subset (a \wedge b)$ soit stricte.

Exercice 23 Soit K un corps. Montrer que le sous-anneau $K[X^2, X^3]$ de $K[X]$ engendré par X^2 et X^3 n'est pas factoriel.

Exercice 24 L'anneau $A = \mathbb{Z}[i\sqrt{3}]$ est-il factoriel ? Et l'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$?

Exercice 25 Soit A un anneau commutatif intègre et soit K son corps des fractions. On dit qu'un élément x de K est entier sur A s'il existe un polynôme $P = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + X^n$ à coefficients dans A tels que $P(x) = 0$.

1) Montrer que si A est factoriel, les éléments de K entiers sur A sont les éléments de A. On dit alors que A est intégralement clos.
2) Dans l'exercice 1, nous avons vu que l'égalité $2 \cdot 2 = (3 + \sqrt{5})(3 - \sqrt{5})$ prouve la non factorialité de $\mathbb{Z}[\sqrt{5}]$. Par contre, elle ne permet pas de déterminer si l'anneau $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ est factoriel ou non. Les questions qui suivent visent à expliquer ce phénomène.
   a) Montrer que $\mathbb{Z}[\sqrt{5}]$ n'est pas intégralement clos.
   b) Montrer que $\frac{1+\sqrt{5}}{2}$ appartient au corps des fractions de $\mathbb{Z}[\sqrt{5}]$ et est entier sur $\mathbb{Z}[\sqrt{5}]$.
   c) Montrer que $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ est intégralement clos.
   d) Mieux, montrer que $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ est euclidien, donc principal, donc factoriel.

   Des phénomènes analogues expliquent les résultats de l'exercice 24 : l'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ est intégralement clos alors que l'anneau $\mathbb{Z}[i\sqrt{3}]$ ne l'est pas.
3) Dans l'exercice 2, nous avons vu que l'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel. Vérifier que ce résultat ne s'explique pas par le fait que $\mathbb{Z}[i\sqrt{5}]$ soit non intégralement clos.

Exercice 26 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.
4) Vérifier que B est intégralement clos mais que A ne l'est pas.

Remarque : Dans B, on peut montrer que tout idéal s'écrit comme produit d'idéaux premiers de manière unique à l'ordre près. Le même résultat valait pour l'anneau $\mathbb{Z}[i\sqrt{5}]$ de l'exercice 2. Ce n'est pas un hasard que ces deux anneaux, qui sont intégralement clos, vérifient cette propriété.

Exercice 27

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 $up_1 \ldots p_n$ 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 28

1) Soit k un corps et considérons l'anneau des séries formelles $k[[X]]$. Montrer que c'est un anneau principal. Montrer que ses idéaux sont $\{0\}$ et les $I_m = (X^m)$ pour chaque $m \in \mathbb{N}$. (On pourra montrer que l'ensemble des éléments non inversibles de $k[[X]]$ est un idéal et que c'est donc le seul idéal maximal).

2) Exhiber un élément de $\mathbb{Z}[X]$ qui n'est pas irréductible, mais qui est irréductible dans $\mathbb{Z}[[X]]$.

3) Exhiber un élément irréductible de $\mathbb{Z}[X]$, mais qui n'est pas irréductible dans $\mathbb{Z}[[X]]$.

Remarque : Les questions concernant la factorialité de $A[[T]]$ sont difficiles. Pierre Samuel a montré en 1960 les faits suivants :

— *Si A est un anneau principal et n un entier naturel, alors l'anneau $A[[T_1, T_2, ..., T_n]]$ est factoriel ;*

— *Il existe des anneaux factoriels A tels que $A[[T]]$ n'est pas factoriel : par exemple, $A = \mathbb{Z}/2\mathbb{Z}[X, Y, Z]/(Z^2 - X^3 - Y^7)$.*

Exercice 29 Soit A un anneau factoriel tel que tout idéal premier non nul est maximal.

1) Soient x, y des éléments non nuls de A, que l'on suppose premiers entre eux. Montrer qu'il existe $u, v \in A$ vérifiant $ux + vy = 1$.

2) Soit I un idéal non nul de A. Montrer qu'il existe $d \in I$ non nul qui est un pgcd de tous les éléments de I.

3) Conclure que A est principal.