Arithmétique des anneaux

1 Anneaux et morphismes

Exercice 1 Soit $n > 0$ un entier.

1) a) Quels sont les diviseurs de 0 de $\mathbb{Z}/n\mathbb{Z}$?
   b) À quelle condition sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il intègre ?
2) a) Quels sont les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$?
   b) On dit qu'un anneau est réduit s'il n'a pas de nilpotents autres que 0. À quelle condition sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il réduit ?
3) Soit $m > 0$ un entier. Quels sont les morphismes d'anneaux :
   a) de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$?
   b) de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$?
   c) de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$?
   d) de $\mathbb{Q}$ dans $\mathbb{Z}/n\mathbb{Z}$?

Exercice 2 Le but de cet exercice est de calculer le groupe des unités de l'anneau $\mathbb{Z}[\sqrt{2}]$.

1) Vérifier que $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{R}$.
2) Vérifier que $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}, \quad a + b\sqrt{2} \mapsto a^2 - 2b^2$ est multiplicative. En déduire que les unités de $\mathbb{Z}[\sqrt{2}]$ sont les $a + b\sqrt{2}$ tels que $N(a + b\sqrt{2}) = a^2 - 2b^2 = \pm 1$.
3) Montrer que $(1 + \sqrt{2})^n$ est une unité pour tout $n \in \mathbb{Z}$.
4) Montrer que $1 + \sqrt{2}$ est la plus petite (pour l'ordre usuel de $\mathbb{R}$) unité de $\mathbb{Z}[\sqrt{2}]$ qui soit strictement plus grande que 1.
5) Montrer que $\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1 + \sqrt{2})^k,\ k \in \mathbb{Z}\}$.

Exercice 3 Soit A un anneau commutatif.

1) On suppose A intègre.
   a) Si A est intègre, montrer que l'anneau $A[X]$ des polynômes à une indéterminée à coefficients dans A est aussi intègre.
   b) Si A est intègre, quelles sont les unités de $A[X]$?
2) On ne suppose plus A intègre.
   a) On rappelle qu'un élément a de A est dit nilpotent s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$. Soit a un élément nilpotent de A, et soit u une unité de A. Montrer que $u + a$ est inversible.

b) Soit $P = a_0 + a_1X + \ldots + a_NX^N$ un polynôme à coefficients dans A. On suppose que a_0 est inversible et que les éléments $a_1, \ldots, a_N$ sont nilpotents. Montrer que P est inversible dans $A[X]$.

c) Réciproquement, montrer que les les unités de $A[X]$ sont les polynômes $P = a_0 + a_1X + \ldots + a_NX^N$ avec a_0 inversible et $a_1, \ldots, a_N$ nilpotents.

d) Dans $(\mathbb{Z}/324\mathbb{Z})[X]$, combien de polynômes de degré n sont des unités ?

Exercice 4 Montrer que tout anneau commutatif intègre fini est un corps.

2 Sous-anneaux et idéaux

Exercice 5 Soit A un anneau commutatif.

1) Supposons que A s'écrit sous la forme $A_1 \times .... \times A_n$ où $A_1, ..., A_n$ sont des anneaux non nuls. Montrer que A possède des idempotents non nuls $e_1, ..., e_n$ tels que $e_ie_j = 0$ pour $i \neq j$ et $e_1 + ... + e_n = 1$.
2) Réciproquement, montrer que si A possède des idempotents non nuls $e_1, ..., e_n$ tels que $e_ie_j = 0$ pour $i \neq j$ et $e_1 + ... + e_n = 1$, alors A s'écrit sous la forme $A_1 \times .... \times A_n$ où $A_1, ..., A_n$ sont des anneaux non nuls. Décrire alors les idéaux de A.
3) Soit $m > 0$ un entier. Quel est le plus grand entier n tel qu'il existe des anneaux non nuls $A_1, ..., A_n$ vérifiant $\mathbb{Z}/m\mathbb{Z} = A_1 \times ... \times A_n$?

Exercice 6 Soient $a, b \in \mathbb{Z}$. Donner des générateurs de $(a) + (b)$, de $(a)(b)$ et de $(a) \cap (b)$.

Exercice 7 Soient A un anneau commutatif et I un idéal de A. On appelle radical de I l'ensemble $\sqrt{I} = \{a \in A | \exists n \in \mathbb{N}^*, a^n \in I\}$.

1) Montrer que $\sqrt{I}$ est un idéal.
2) Reconnaître $\sqrt{A}$ et $\sqrt{(0)}$.
3) Soit J un idéal de A. Déterminer si les assertions suivantes sont vraies ou fausses. Corriger celles qui sont fausses.
   (a) $\sqrt{\sqrt{I}} = \sqrt{I}$.
   (b) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
   (c) $\sqrt{IJ} = \sqrt{I} \cdot \sqrt{J}$.
   (d) $\sqrt{I + J} = \sqrt{I} + \sqrt{J}$.
4) Prenons $A = \mathbb{Z}$ et $I = N\mathbb{Z}$. Calculer $\sqrt{I}$.

Exercice 8 Soient A un anneau commutatif et I et J deux idéaux.

1) On suppose que $I + J = A$. Montrer que $I^n + J^n = A$ pour tout $n > 0$.

2) On suppose que $I+J=A$. Soit L un idéal tel que $IL \subseteq J$. Montrer que $L \subseteq J$.
3) On suppose que $I \cap J = IJ$. A-t'on forcément $I+J=A$?

3 Quotients d'anneaux

Exercice 9

1) Montrer que l'anneau $\mathbb{Z}[i]$ est isomorphe à $\mathbb{Z}[X]/(X^2+1)$.
2) Réaliser les anneaux $\mathbb{Z}[i\sqrt{7}]$ et $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ comme quotients de $\mathbb{Z}[X]$.

Exercice 10 Soit k un corps.

1) Montrer que la k-algèbre $k[X,Y]/(X^2-Y^3)$ est isomorphe à $k[T^2,T^3]$.
2) Montrer que la k-algèbre $k[X,Y]/(X^2-Y)$ est isomorphe à $k[T]$.
3) Plus généralement, soient a et b deux entiers naturels non nuls. Réaliser l'anneau $k[T^a,T^b]$ comme quotient de $k[X,Y]$.
4) Montrer que la k-algèbre $k[X,Y]/(XY-1)$ n'est pas isomorphe à $k[T]$.

Exercice 11 On considère les anneaux :

$$\mathbb{C}[X], \mathbb{R}[X]/(X^2+X+1), \mathbb{R}[X]/(X^3-6X^2+11X-6), \mathbb{R}[X]/(X^4-1), \mathbb{R}[X]/(X^5).$$

Déterminer les morphismes de $\mathbb{R}$-algèbres de ces algèbres à valeurs dans $\mathbb{R}$ (resp. $\mathbb{C}$).

4 Idéaux premiers et maximaux

Exercice 12 Soit p un nombre premier et soit $\alpha = i\sqrt{p}$. On considère l'anneau $A = \mathbb{Z}[\alpha]$. Montrer que l'idéal (α) de A est $\{a+b\alpha | a \in p\mathbb{Z},\ b \in \mathbb{Z}\}$. Est-il premier? Est-il maximal?

Exercice 13 Soit A un anneau commutatif. Montrer l'égalité

$$\bigcup_{\mathfrak{M} \text{ idéal maximal de } A} \mathfrak{M} = A \smallsetminus A^\times.$$

Exercice 14 Soient $f : A \to B$ un morphismes d'anneaux commutatifs. Montrer que l'image réciproque d'un idéal premier de B est un idéal premier de A. Est-ce encore vrai pour un idéal maximal?

Exercice 15 Soient A un anneau commutatif et I un idéal.

1) Montrer que les idéaux de A/I sont en bijection avec les idéaux de A contenant I.

2) Soit $J \supseteq I$ un idéal de A. Montrer que A/J est canoniquement isomorphe au quotient de A/I par J/I.
3) On dit que I est un idéal premier (resp. maximal) si A/I est intègre (resp. un corps). Montrer que les idéaux premiers (resp. maximaux) de A/I sont en bijection avec les idéaux premiers (resp. maximaux) de A contenant I.
4) Soit $n > 0$ un entier. Quels sont les idéaux de $\mathbb{Z}/n\mathbb{Z}$? Lesquels sont premiers ? Et maximaux ?
5) Déterminer les idéaux des anneaux suivants :

$$\mathbb{R}[X]/(X^2+X+1), \mathbb{R}[X]/(X^3-6X^2+11X-6), \mathbb{R}[X]/(X^4-1), \mathbb{R}[X]/(X^5).$$

Lesquels sont premiers ? Et maximaux ?
6) Combien l'anneau $\mathbb{R}[X]/(X^5(X^4-1))$ possède-t'il d'idéaux ? d'idéaux premiers ? d'idéaux maximaux ?

Exercice 16 On considère l'anneau $A = \mathbb{Z}[\sqrt{7}]$. L'idéal (3) est-il premier ? Et l'idéal (5) ?

Exercice 17 Soit A un anneau commutatif.

1) On suppose que A est intègre et ne possède qu'un nombre fini d'idéaux. Montrer que A est un corps.
2) On suppose que A ne possède qu'un nombre fini d'idéaux. Montrer que tout idéal premier est maximal.
3) On suppose que tout idéal propre de A est premier. Montrer que A est un corps.

Exercice 18 Soit A un anneau commutatif.

1) Soient $\mathfrak{p}$ un idéal premier et $I_1, ..., I_n$ des idéaux. On suppose que $\mathfrak{p}$ contient $\prod_{k=1}^n I_k$. Montrer que $\mathfrak{p}$ contient l'un des I_k.
2) Soient I un idéal et $\mathfrak{p}_1, ..., \mathfrak{p}_n$ des idéaux premiers. On suppose que I est contenu dans $\bigcup_{k=1}^n \mathfrak{p}_k$. Montrer que I est contenu dans l'un des $\mathfrak{p}_k$.

Exercice 19

1) Soient A un anneau commutatif et I un idéal de A. Notons J l'intersection des idéaux premiers de A contenant I. Le but de cette question est de montrer que $\sqrt{I} = J$.
   (a) Montrer que $\sqrt{I}$ est contenu dans J.
   (b) Réciproquement, soit $a \in A \smallsetminus \sqrt{I}$, et considérons $\mathscr{E}$ la famille constituée des idéaux qui contiennent I mais qui ne contiennent aucune puissance de a. Montrer que $\mathscr{E}$ possède un élément maximal (pour l'inclusion), qui est un idéal premier de A. En déduire que $a \notin J$.
   (c) Conclure.

Soit $\mathscr{C}$ l'anneau des fonctions continues de $[0,1]$ dans $\mathbb{R}$.

2) Montrer que les idéaux maximaux de $\mathscr{C}$ sont les

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

pour $x \in [0,1]$.

3) Soit $I = \{f \in \mathscr{C} \mid \forall m \in \mathbb{N}, \lim_{x\to 0} \frac{f(x)}{x^m} = 0\}$. Montrer que $I = \sqrt{I}$ (on dit que I est un idéal radical). L'idéal I est-il premier?

4) En déduire que $\mathscr{C}$ possède des idéaux premiers non maximaux.

5 Unités de $\mathbb{Z}/n\mathbb{Z}$

Exercice 20 Dans cet exercice, nous voulons étudier la structure du groupe des unités d'un groupe cyclique. On rappelle que tout sous-groupe fini du groupe des unités d'un corps est cyclique. Cela entraîne en particulier que $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ pour tout nombre premier p.

1) Rappeler quel est l'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$.

2) Soient p un nombre premier impair et $m > 1$ un entier.

   (a) Montrer que $(1+p)^{p^{m-2}} \equiv 1 + p^{m-1} \mod p^m$, puis que $1+p$ est d'ordre p^{m-1} dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$.

   (b) En déduire que le noyau de la projection naturelle $(\mathbb{Z}/p^m\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/p^{m-1}\mathbb{Z}$.

   (c) Montrer qu'il existe $x_0 \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ d'ordre $p-1$.

   (d) Montrer que $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z} \to (\mathbb{Z}/p^m\mathbb{Z})^\times, (a,b) \mapsto x_0^a(1+p)^b$ est un isomorphisme. En déduire que $(\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^{m-1}\mathbb{Z}$.

3) Soit $m > 2$ un entier.

   (a) Montrer que $5^{2^{m-3}} \equiv 1+2^{m-1} \mod 2^m$, puis que 5 est d'ordre 2^{m-2} dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$.

   (b) En déduire que le noyau de la projection naturelle $(\mathbb{Z}/2^m\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/2^{m-2}\mathbb{Z}$.

   (c) En s'inspirant de la question 2.(d), montrer que $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

4) Quelle est la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$? Quand ce groupe est-il cyclique?

Exercice 21

1. Donner un générateur du groupe $(\mathbb{Z}/162\mathbb{Z})^\times$.
2. Donner un élément d'ordre maximal dans $(\mathbb{Z}/2592\mathbb{Z})^\times$.

6 Divisibilité dans les anneaux

Exercice 22 Soit $A = \mathbb{Z}[\sqrt{5}]$. On considère l'application $N : A \to \mathbb{Z}, z = a + b\sqrt{5} \mapsto a^2 - 5b^2$.

1) Montrer qu'un élément z de A est inversible si, et seulement si, $N(z) = \pm 1$. Vérifier 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 (à l'ordre et à association près) 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 45 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 23 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 (à l'ordre et à association près) de la décomposition de 21 en facteurs irréductibles dans A.
4) Faire la liste des idéaux premiers de A contenant 3 et celle des idéaux premiers de A contenant 7. Exhiber des idéaux premiers $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{q}_1, \mathfrak{q}_2$ tels que :

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

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 24 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.

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

7 Anneaux euclidiens et principaux

Exercice 25 Exhiber un idéal non principal de $\mathbb{Z}[i\sqrt{5}]$.

Exercice 26 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 27 Soit A un anneau commutatif. Montrer que si A n'est pas un corps, alors $A[X]$ n'est pas principal.

Exercice 28 Soit $\mathscr{C}$ (resp. $\mathscr{C}^\infty$) l'anneau des fonctions continues (resp. C^∞) de $[0,1]$ dans $\mathbb{R}$.

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

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

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

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

Exercice 29 Trouver tous les couples $(x,y) \in \mathbb{Z}^2$ tels que $y^2 = x^3 + 16$.

Exercice 30 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 31 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 32 Factoriser $-3 + 15i$ en irréductibles dans $\mathbb{Z}[i]$.

Exercice 33 En utilisant l'exercice 30, trouver toutes les seules solutions entières de l'équation $y^2 + 4 = x^3$.

Exercice 34 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 35 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 36 Factoriser $9 + 3j + 6j^2$ en irréductibles dans $\mathbb{Z}[j]$.

Exercice 37 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 34.

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 38 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 39 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 40 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).

8 Anneaux factoriels

Exercice 41 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 42 Soit K un corps. Montrer que la sous-K-algèbre $K[X^2, X^3]$ de $K[X]$ engendré par X^2 et X^3 n'est pas factoriel.

Exercice 43 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 44 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.

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 23. Ces anneaux ont des propriétés similaires que nous allons étudier en détail dans la suite du cours. Il se comportent par contre différemment de l'anneau A.

Exercice 45 Montrer que l'anneau $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ est factoriel.

Exercice 46

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) Montrer que $\mathbb{Z}[\sqrt{6}]$ est factoriel.

Exercice 47

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 48 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.

9 Anneaux de polynômes

Exercice 49 Soit A un anneau principal de corps des fractions K. Nous allons caractériser les idéaux premiers et maximaux de $A[X]$.

1) Soit I un idéal premier non nul de $A[X]$.
   a) Montrer que $I \cap A$ est un idéal maximal de A.
   b) On suppose $I \cap A = 0$.
      i) Soit J l'idéal de $K[X]$ engendré par I. Montrer que $I = J \cap A[X]$.
      ii) Montrer que I est principal, engendré par un polynôme non constant, irréductible et primitif.
   c) On suppose que $I \cap A$ est non nul, et on pose $k = A/(I \cap A)$. Montrer que soit I est engendré par $I \cap A$, soit I est engendré par $I \cap A$ et par un polynôme $P \in A[X]$ dont l'image dans $k[X]$ est irréductible.
   d) Déduire de ce qui précède que les idéaux premiers de $A[X]$ sont : (0) ; les idéaux principaux engendrés par un polynôme non constant, irréductible et primitif ; les idéaux engendrés par un idéal maximal de A ; les idéaux engendrés par un idéal maximal $\mathfrak{m}$ de A et un polynôme de $A[X]$ dont la réduction modulo $\mathfrak{m}$ est irréductible. Lesquels sont maximaux ?
2) Quels sont les idéaux premiers (resp. maximaux) de $\mathbb{C}[X,Y]$?
3) Quels sont les idéaux premiers (resp. maximaux) de $\mathbb{Z}[X]$?
4) Soit α un entier algébrique, c'est-à-dire un élément de $\mathbb{C}$ racine d'un polynôme unitaire irréductible à coefficients dans $\mathbb{Z}$. Montrer que tout idéal premier non nul de $\mathbb{Z}[\alpha]$ est maximal.

Exercice 50 On considère le polynôme :

$$P(X) = X^5 - 11X^3 - 3X^2 + 34X - 21.$$

1. Trouver toutes les racines rationnelles de P.
2. Ecrire P comme produit de polynômes irréductibles sur $\mathbb{C}$, $\mathbb{R}$ et $\mathbb{Q}$.

Exercice 51 On considère le polynôme :

$$P(X) = 5X^5 - 2X^4 + 10X^2 + 6X - 4.$$

1. Trouver toutes les racines rationnelles de P.
2. Ecrire P comme produit de polynômes irréductibles sur $\mathbb{Q}$.

Exercice 52 On considère les polynômes :

$$P(X) = 3X^3 + X^2 + X - 2, \quad Q(X) = 2X^3 + 3X + 3,$$
$$R(X) = X^5 + 78X^4 - 117X^2 + 234, \quad S(X) = X^5 - 4X^2 - 10X + 4.$$

Sont-ils irréductibles sur $\mathbb{Q}$?

Exercice 53 Montrer que si p est un nombre premier, le polynôme cyclotomique $\Phi_p(X) = X^{p-1} + \cdots + X + 1 = \frac{X^p-1}{X-1}$ est irréductible dans $\mathbb{Q}[X]$ (*Indication :* on pourra poser $X = Y + 1$).

10 Vrai ou faux de révision du chapitre 1

Exercice 54 Soit A un anneau commutatif. Décider si les affirmations suivantes sont vraies ou fausses.

1) Si a, b et u sont trois éléments A tels que $(a) = (b)$ et $a = bu$, alors $u \in A^\times$.
2) Si A est intègre, I est un idéal principal et A/I est un anneau principal, alors A est principal.
3) Dans $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$, l'idéal (3) n'est pas premier, mais il est contenu dans exactement deux idéaux premiers, qui sont maximaux.
4) Tout idéal du quotient d'un anneau principal par un idéal est principal.
5) La somme de deux idéaux non principaux d'un anneau est soit un idéal non principal soit l'anneau tout entier.
6) L'idéal (89) est premier dans $\mathbb{Z}[i]$.
7) L'anneau des nombres décimaux est isomorphe à $\mathbb{Z}[X]/(10X-1)$.
8) L'anneau des nombres décimaux est euclidien.
9) Les groupes $\mathbb{Q}^\times$ et $(\mathbb{F}_3(X))^\times$ sont isomorphes.
10) Un sous-anneau d'un anneau euclidien est factoriel.
11) Si A est factoriel, alors tout idéal premier non nul est maximal.
12) Le quotient d'un anneau factoriel par un idéal premier est factoriel.
13) Si A est un anneau factoriel et a et b sont des éléments non nuls de A, on a $(a,b) = (a \wedge b)$.
14) Si A est un anneau factoriel et a et b sont des éléments non nuls de A, on a $(a) \cap (b) = (a \vee b)$.
15) L'anneau $\mathbb{Z}[(X_n)_{n\in\mathbb{N}}]$ est factoriel.
16) Le polynôme $(X-1)^{73} + 74 \in \mathbb{Q}[X]$ est irréductible.
17) Il existe un morphisme d'anneaux injectif de $\mathbb{Z}[X]/(2X^2+3X+2)$ dans $\mathbb{C}$.
18) Si A est intègre, tout élément irréductible engendre un idéal premier.
19) Si A est factoriel et si a et b sont deux éléments de A premiers entre eux, alors il existe un isomorphisme $A/(ab) \cong A/(a) \times A/(b)$.
20) Si $P \in \mathbb{C}[X,Y]$ est tel que $P(X,0)$ et $P(0,Y)$ sont irréductibles, alors P est irréductible.