Université d'Angers – 2025/2026

Théorie des anneaux

1 Généralités sur les anneaux

Exercice 1. Soit $d \in \mathbb{Z}$. Si $d < 0$, on note $\sqrt{d} \coloneqq i\sqrt{-d}$.

1. Montrer que $\left\{ a + b\sqrt{d} \ : \ a, b \in \mathbb{Z} \right\}$ est le plus petit sous-anneau de $\mathbb{C}$ contenant $\sqrt{d}$.
2. Montrer que $\left\{ a + b\sqrt{d} \ : \ a, b \in \mathbb{Q} \right\}$ est le plus petit sous-corps de $\mathbb{C}$ contenant $\sqrt{d}$.
3. (a) Montrer que si $d \equiv 1 \mod 4$ alors $\left\{ a + \frac{1+\sqrt{d}}{2} b \ : \ a, b \in \mathbb{Z} \right\}$ est un anneau.

   Indice : on pourra remarquer que $\frac{1+\sqrt{d}}{2}$ est solution d'un polynôme quadratique à coefficients entiers.

   (b) Est-ce toujours vrai si $d \not\equiv 1 \mod 4$?

Exercice 2. Soient A un anneau et $a \in A$.
Montrer que s'il existe $b, c \in A$ tels que $ab = ca = 1$ alors a est inversible.

Exercice 3.

1. Est-ce que l'application trace $\mathrm{tr} : M_2(\mathbb{R}) \to \mathbb{R}$ est un morphisme d'anneaux ?
2. Est-ce que l'application déterminant $\det : M_2(\mathbb{R}) \to \mathbb{R}$ est un morphisme d'anneaux ?

Exercice 4. Soit $f : A \to B$ un morphisme d'anneaux.

1. Montrer que si A est trivial alors B est trivial.
2. La réciproque est-elle vraie ?
3. Montrer que si B est non trivial alors $\ker(f)$ n'est pas un sous-anneau de A.

Exercice 5. Soit $(A, +, \cdot, 0, 1)$ un anneau. On définit $\oplus : A \times A \to A$ et $\odot : A \times A \to A$ par

$$a \oplus b \coloneqq a + b + 1 \qquad \text{et} \qquad a \odot b \coloneqq ab + a + b.$$

1. Montrer que $\oplus$ admet un neutre que l'on note e et que $\odot$ admet un neutre que l'on note u.
2. Montrer que $(A, \oplus, \odot, e, u)$ est un anneau isomorphe à $(A, +, \cdot, 0, 1)$.
   Indice : on pourra commencer par exhiber une bijection $\varphi : A \to A$ compatible avec les lois.

Exercice 6. Déterminer, à isomorphisme près, tous les anneaux à 2 (resp. 3) éléments.

Exercice 7. Trouver une condition nécessaire et suffisante sur $n, m \in \mathbb{N}$ pour qu'il existe un morphisme d'anneaux $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

Exercice 8 (Anneaux de polynômes – **très important**)**.**
Soit A un anneau. On définit l'ensemble des *polynômes à coefficients dans A*, noté $A[X]$, comme l'ensemble des suites d'éléments de A à support fini, i.e.

$$\forall (a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}},\ (a_n)_{n\in\mathbb{N}} \in A[X] \Leftrightarrow \left(\exists N \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geq N \implies a_n = 0\right).$$

Pour $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in A[X]$, on définit

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} \coloneqq (a_n + b_n)_{n\in\mathbb{N}}$$

et

$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} \coloneqq \left(\sum_{k=0}^{n} a_k b_{n-k} \right)_{n\in\mathbb{N}}.$$

On pose $0 \coloneqq (0, 0, \ldots) \in A[X]$ et $1 \coloneqq (1, 0, 0, \ldots) \in A[X]$. Pour $P \coloneqq (a_n)_{n\in\mathbb{N}} \in A[X] \setminus \{0\}$, on définit le *degré* de P par $\deg(P) \coloneqq \max\left\{ n \in \mathbb{N} \ : \ a_n \neq 0 \right\}$ et on pose $\deg(0) \coloneqq -\infty$.

1. Montrer que $(A[X], 0, 1, +, \cdot)$ est un anneau.
2. (a) Montrer que $\iota : A \to A[X]$ défini par $\iota(a) = (a, 0, 0, \ldots)$ est un morphisme d'anneaux injectif.

   (b) Montrer que pour $(a_n)_{n\in\mathbb{N}} \in A[X]$, on a $(a_n)_{n\in\mathbb{N}} = \sum_{n\geq 0} a_n X^n$ où $X \coloneqq (0, 1, 0, 0, \ldots \ldots)$ et, pour $n \in \mathbb{N}$, on identifie $a_n \in A$ avec $\iota(a_n) \coloneqq (a_n, 0, 0, \ldots) \in A[X]$.

3. Montrer que A est commutatif si et seulement si $A[X]$ l'est.
4. On suppose que A est un anneau commutatif non trivial.
   (a) Montrer que si le coefficient dominant de $g \in A[X] \setminus \{0\}$ n'est pas un diviseur de zéro dans A alors $\forall f \in A[X]$, $\deg(fg) = \deg(f) + \deg(g)$.
   (b) Montrer que les propriétés suivantes sont équivalentes :
      (i) $A[X]$ est intègre
      (ii) A est intègre
      (iii) $\forall f, g \in A[X]$, $\deg(fg) = \deg(f) + \deg(g)$
5. On suppose maintenant que A un anneau commutatif.
   (a) Soient $f, g \in A[X]$ tels que $g \neq 0$ et que le coefficient dominant de g est inversible dans A. Montrer qu'il existe $q, r \in A[X]$ uniquement déterminés par $f = qg + r$ et $\deg(r) < \deg(g)$. *On appelle q et r le* quotient *et le* reste *de la* division euclidienne *de f par g.*
   (b) Soient $f \in A[X]$ et $a \in A$. Montrer que a est une racine de f si et seulement s'il existe $g \in A[X]$ tel que $f = (X - a)g$.
   (c) On suppose maintenant que A est un anneau commutatif non trivial. Montrer que A est intègre si et seulement si tout polynôme non nul $f \in A[X]$ possède au plus $\deg(f)$ racines.

Exercice 9. Les sous-ensembles suivants sont-ils des sous-anneaux de $\mathbb{Z}[X]$?

1. $\left\{P \in \mathbb{Z}[X] \ : \ \deg(P) \leq n\right\}$ où $n \in \mathbb{N}$
2. $\left\{P \in \mathbb{Z}[X] \ : \ \deg(P) \equiv 0 \mod 2\right\} \cup \{0\}$
3. $\{XQ \ : \ Q \in \mathbb{Z}[X]\}$
4. $\left\{P(X^2) \ : \ P \in \mathbb{Z}[X]\right\}$

Exercice 10. Les applications suivantes sont-elles des morphismes d'anneaux ?

1. $\begin{array}{ccc} \mathbb{Z}[X] & \to & \mathbb{Z} \\ P & \mapsto & P(1) \end{array}$
2. $\begin{array}{ccc} \mathbb{Z}[X] & \to & \mathbb{Z} \\ P & \mapsto & P'(0) \end{array}$

Exercice 11 (**Très important**)**.**

1. Soient A un anneau commutatif, B un sous-anneau de A et $\omega \in A$.
   (a) Montrer que $\mathrm{ev}_\omega : B[X] \to A$, défini par $\mathrm{ev}_\omega\left(\sum_{k=0}^{d} a_k X^k\right) \coloneqq \sum_{k=0}^{d} a_k \omega^k$, est un morphisme d'anneaux. Pour $P \in B[X]$, on note $P(\omega) \coloneqq \mathrm{ev}_\omega(P)$.
   (b) On pose $B[\omega] \coloneqq \{P(\omega) \ : \ P \in B[X]\}$. Montrer que $B[\omega]$ est le plus petit sous-anneau de A contenant B et ω.
2. On considère maintenant $A = \mathbb{C}$. Soit $\omega \in \mathbb{C}$.
   (a) Montrer que $\mathbb{Z}[\omega]$ est le plus petit sous-anneau de $\mathbb{C}$ contenant ω.
   (b) On suppose qu'il existe $P \in \mathbb{Z}[X]$ unitaire de degré $d \geq 1$ tel que $P(\omega) = 0$. Montrer que $\mathbb{Z}[\omega] = \left\{a_{d-1}\omega^{d-1} + \cdots + a_1\omega + a_0 \ : \ a_0, a_1, \ldots, a_{d-1} \in \mathbb{Z}\right\}$.
   (c) Le résultat de la question précédente reste-t-il vrai si on ne suppose pas P unitaire ?
   (d) Soit $d \in \mathbb{Z}$, déterminer explicitement $\mathbb{Z}\left[\sqrt{d}\right]$ et $\mathbb{Q}\left[\sqrt{d}\right]$ où $\sqrt{d} \coloneqq i\sqrt{d}$ si $d < 0$.

Exercice 12. Parmi les anneaux suivants, lesquels sont intègres ?

1. $\mathbb{Q}$
2. $\mathbb{Z}[i]$
3. $\mathbb{Z}/6\mathbb{Z}$
4. $\mathbb{Z}/7\mathbb{Z}$
5. $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$

Exercice 13.

1. Montrer que si z est l'inverse de $1 - yx$ alors $z - 1 = yxz = zyx$.
2. En déduire qu'il existe $t \in A$ tel que $t - 1 = xyt = txy$.
3. Conclure que $1 - xy$ est inversible.

Exercice 14. Montrer qu'un anneau intègre fini est un corps.

Exercice 15 (L'anneau $\mathbb{H}$ des quaternions)**.**

1. Montrer que $\mathbb{H} \coloneqq \left\{ \begin{pmatrix} z_1 & -z_2 \\ \overline{z_2} & \overline{z_1} \end{pmatrix} \ : \ z_1, z_2 \in \mathbb{C} \right\} \subset M_2(\mathbb{C})$ est un anneau à division non commutatif.
2. Montrer que $X^2 + 1 \in \mathbb{H}[X]$ a une infinité de racines.

Exercice 16.
On définit le *centre* d'un anneau A par $C(A) \coloneqq \{x \in A \ : \ \forall a \in A,\ xa = ax\}$.

1. Montrer que le centre $C(A)$ est un sous-anneau de A.
2. Déterminer le centre $C(\mathbb{H})$ de $\mathbb{H}$.
   Indice : on pourra considérer $I \coloneqq \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ *et* $J \coloneqq \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Exercice 17.
Soit A un *anneau de Boole*, i.e. vérifiant $\forall a \in A,\ a^2 = a$.

1. Montrer $\forall a \in A,\ 2a = 0$.
2. Montrer que A est commutatif.
3. Montrer que 0 est le seul élément nilpotent de A.
4. Montrer que 1 est le seul élément inversible de A.
5. On suppose que A est intègre, déterminer A.

Exercice 18.
Soit E un ensemble.

1. Montrer que $(\mathbb{Z}/2\mathbb{Z})^E$ est un anneau de Boole.
2. Montrer que $\varphi : \begin{array}{ccc} (\mathbb{Z}/2\mathbb{Z})^E & \to & \mathcal{P}(E) \\ f & \mapsto & f^{-1}(1) \end{array}$ est bijective.
3. En déduire que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau de Boole.
   On rappelle que la *différence symétrique* de $A, B \in \mathcal{P}(E)$ est définie par $A \Delta B \coloneqq (A \cup B) \setminus (A \cap B)$.

Exercice 19.

1. (a) Montrer que $\forall a, b \in \mathbb{Z},\ a + b\sqrt{2} = 0 \Leftrightarrow a = b = 0$.
   (b) En déduire que $\forall a, b, c, d \in \mathbb{Z},\ a + b\sqrt{2} = c + d\sqrt{2} \Leftrightarrow a = c$ et $b = d$.
2. On considère $A \coloneqq \mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \ : \ a, b \in \mathbb{Z}\right\}$.
   Pour $a, b \in \mathbb{Z}$, on note $N\left(a + b\sqrt{2}\right) \coloneqq a^2 - 2b^2$.
   (a) Montrer que $\forall z, z' \in A,\ N(zz') = N(z)N(z')$.
   (b) Montrer que $\forall z \in A,\ z \in A^* \Leftrightarrow |N(z)| = 1$.
   (c) On définit $W \coloneqq \left\{z \in A^* \ : \ z > 1\right\}$.
   Montrer que si $a + b\sqrt{2} \in W$ alors $-1 < a - b\sqrt{2} < 1$.
   (d) En déduire que si $a + b\sqrt{2} \in W$ alors $a, b > 0$.
   (e) Montrer que W admet un plus petit élément, que l'on note $\omega \coloneqq \min(W)$ dans la suite.
   (f) Soit $z \in A^* \cap]0, +\infty[$.
      i. Montrer qu'il existe un entier $n \in \mathbb{Z}$ tel que $\omega^{n-1} < z \leq \omega^n$.
      ii. Montrer que $z = \omega^n$.
   (g) Déterminer A^*.

2 Idéaux & passage au quotient

Exercice 20.
On considère $C^0([0,1])$ l'anneau des fonctions $f : [0,1] \to \mathbb{R}$ continues.
Montrer de deux façons différentes que $I \coloneqq \left\{f \in C^0([0,1]) \ : \ f(0) = 0\right\}$ est un idéal de $C^0([0,1])$.
Indication : pour la première méthode, on pourra utiliser la définition, et pour la seconde, remarquer que I est le noyau d'un morphisme d'anneaux.

Exercice 21. Montrer que les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Exercice 22.
Soit $f : A \to B$ un morphisme d'anneaux.

1. Montrer que si f est surjectif alors l'image d'un idéal de A par f est un idéal de B.
2. Le résultat de la question précédente reste-t-il vrai si on ne suppose pas f surjectif ?

Exercice 23.

1. Montrer qu'un anneau à division A possède exactement deux idéaux, à savoir $\{0\}$ et A.
2. (a) Montrer que $M_2(\mathbb{Z}/2\mathbb{Z})$ n'est pas un anneau à division.
   (b) Montrer que pour tout $a, b, c, d \in \mathbb{Z}/2\mathbb{Z}$, on a dans $M_2(\mathbb{Z}/2\mathbb{Z})$:
   - $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$
   - $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$
   - $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$

   (c) En déduire que $M_2(\mathbb{Z}/2\mathbb{Z})$ possède exactement deux idéaux.
   (d) Est-ce que la réciproque de l'énoncé de la question (1) est vraie ?
3. Montrer qu'un anneau commutatif est un corps ssi il possède exactement deux idéaux.
4. Soient A un anneau à division, B un anneau et $f : A \to B$ un morphisme d'anneaux.
   (a) Montrer que si B n'est pas trivial alors f est injectif.
   (b) Que se passe-t-il si B est trivial ?

Exercice 24.
On définit l'ensemble des nombres décimaux par $\mathbb{D} \coloneqq \left\{ \frac{a}{10^k} \ : \ a \in \mathbb{Z},\, k \in \mathbb{N} \right\}$.

1. Montrer que $\mathbb{D}$ est un anneau intègre pour les lois usuelles.
2. Déterminer l'ensemble $\mathbb{D}^*$ des inversibles de $\mathbb{D}$.
3. (a) Montrer que si I est un idéal de $\mathbb{D}$ alors $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$.
   (b) En déduire que $\mathbb{D}$ est principal.

Exercice 25.
On considère $I \coloneqq (2, X)$ l'idéal de $\mathbb{Z}[X]$ engendré par 2 et X.

1. Montrer que $I = \{P \in \mathbb{Z}[X] \ : \ P(0) \equiv 0 \mod 2\}$.
2. Est-ce que I est un idéal principal ?

Exercice 26. Soient A un anneau commutatif et I un idéal de A.
On définit le *radical* de I par $\sqrt{I} \coloneqq \left\{ x \in A \ : \ \exists n \in \mathbb{N} \setminus \{0\},\, x^n \in I \right\}$.

1. Montrer que $\sqrt{I}$ est un idéal de A.
2. Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.
3. Déterminer $\sqrt{I}$ pour $A = \mathbb{Z}$ et $I = n\mathbb{Z}$ où $n \in \mathbb{N}$.
4. Montrer que 0 est le seul nilpotent de $A/\sqrt{I}$.

Exercice 27. Pour chacun des anneaux suivants, exhiber un anneau isomorphe "plus simple" :

1. $A[X]/(X - a)$ où A est un anneau commutatif et $a \in A$.
2. $\mathbb{Z}[X]/(2X - 1)$

Exercice 28. *Le but de cet exercice est de démontrer le deuxième théorème d'isomorphisme.*
Soient A un anneau, B un sous-anneau de A et I un idéal de A.

1. Montrer que $B + I$ est un sous-anneau de A.
2. Montrer que $B \cap I$ est un idéal de B.
3. Montrer que I est un idéal de $B + I$.
4. Montrer que les anneaux $B/B \cap I$ et $(B + I)/I$ sont isomorphes.

Exercice 29 (Caractéristique d'un anneau)**.**
Soit A un anneau.

1. Montrer qu'il existe un unique morphisme d'anneaux $\Theta : \mathbb{Z} \to A$.
2. Montrer qu'il existe un unique $c \in \mathbb{N}$ tel que $\ker(\Theta) = c\mathbb{Z}$.

Cet entier c, que l'on note $\mathrm{car}(A)$, est appelé *la caractéristique* de A. C'est le plus petit entier $c > 0$ tel que

$$\underbrace{1 + 1 + \cdots + 1}_{c \text{ fois}} = 0,$$

s'il existe, et sinon $\mathrm{car}(A) = 0$ (on dit alors que A est de *caractéristique nulle*).

3. Déterminer la caractéristique des anneaux suivants :
   (a) $\mathbb{Z}$ (c) $\mathbb{Q}$ (e) $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
   (b) $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}$ (d) $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (f) $\mathbb{Q} \times \mathbb{Z}/4\mathbb{Z}$
4. Montrer que A contient un sous-anneau isomorphe à $\mathbb{Z}/\operatorname{car}(A)\mathbb{Z}$.
5. On suppose dans cette question que $p \coloneqq \operatorname{car}(A)$ est un nombre premier.
   (a) Montrer que $\forall k \in \{1, \dots, p-1\},\ p \mid \binom{p}{k}$.
   (b) Montrer que si $a, b \in A$ vérifient $ab = ba$ alors $(a+b)^p = a^p + b^p$.
   (c) En déduire que si A est commutatif alors $\begin{array}{ccc} A & \to & A \\ a & \mapsto & a^p \end{array}$ est un morphisme d'anneaux.
6. Montrer que si A est intègre alors $\operatorname{car}(A)$ est soit nulle soit un nombre premier.

Exercice 30.
1. Déterminer les idéaux premiers de $\mathbb{Z}$.
2. Déterminer les idéaux maximaux de $\mathbb{Z}$.

Exercice 31.
1. Montrer que tout idéal de $\mathbb{Z}/8\mathbb{Z}$ est principal.
2. L'anneau $\mathbb{Z}/8\mathbb{Z}$ est-il principal ?
3. Montrer que $\mathbb{Z}/8\mathbb{Z}$ admet quatre idéaux que l'on donnera explicitement.
4. Montrer que $\mathbb{Z}/8\mathbb{Z}$ admet un unique idéal premier.

Exercice 32.
L'idéal I de A est-il premier ? maximal ?
1. $A = \mathbb{Q}[X]$, $I = (X^2 - 2)$
2. $A = \mathbb{Z}[X]$, $I = (X^2 - 2)$
3. $A = \mathbb{R}[X]$, $I = (X^2 - 2)$
4. $A = \mathbb{R}[X]$, $I = (X - 2)$
5. $A = \mathbb{R}[X]$, $I = (X^2 + 1)$
6. $A = \mathbb{C}[X]$, $I = (X^2 + 1)$
7. $A = \mathbb{Z}[i]$, $I = (1 + i)$
8. $A = \mathbb{Z}[X]$, $I = (n, X)$ où $n \in \mathbb{N} \setminus \{0\}$

Exercice 33.
Dire si les assertions suivantes sont vraies ou fausses, en justifiant.
1. Soit $f : A \to B$ est un morphisme d'anneaux.
   Si I est un idéal premier de B alors $f^{-1}(I)$ est un idéal premier de A.
2. Soit $f : A \to B$ est un morphisme d'anneaux.
   Si I est un idéal maximal de B alors $f^{-1}(I)$ est un idéal maximal de A.
3. Soient B un anneau et A un sous-anneau de B.
   Si I est un idéal premier de B alors $I \cap A$ est un idéal premier de A.
4. Soient B un anneau et A un sous-anneau de B.
   Si I est un idéal maximal de B alors $I \cap A$ est un idéal maximal de A.

Exercice 34.
On considère l'unique morphisme d'anneaux $\Theta : \mathbb{Z} \to \mathbb{Z}[i]/(i-3)$, i.e. $\Theta(n) \coloneqq \overline{n}$.
1. Montrer que Θ induit un isomorphisme $\theta : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}[i]/(i-3)$ puis déterminer θ^{-1}.
2. L'idéal $(i-3)$ de $\mathbb{Z}[i]$ est-il premier ? maximal ?

Exercice 35.
Soit A un anneau de Boole (voir l'Exercice 17).
1. Montrer que si I est un idéal de A alors A/I est un anneau de Boole.
2. (a) Montrer que si I est un idéal premier de A alors $A/I \simeq \mathbb{Z}/2\mathbb{Z}$.
   (b) En déduire que tout idéal premier de A est maximal.
   (c) Soit I un idéal premier. Montrer que $\forall x, y \in A \setminus I,\ x + y \in I$.
3. (a) Montrer que $\forall x, y \in A,\ (x, y) = (x + y + xy)$.
   (b) En déduire que tout idéal de A finiment engendré est principal.

Exercice 36.
1. Soit A un anneau principal. Montrer que tout idéal premier non nul de A est maximal.
2. L'énoncé de la question précédente est-il vrai si A est un anneau quelconque ?

Exercice 37.
Soit A un anneau. On dit que $a \in A$ est *nilpotent* s'il existe $n \in \mathbb{N} \setminus \{0\}$ tel que $a^n = 0$.
On dénote l'ensemble des nilpotents de A par $\mathrm{Nil}(A)$.

1. Montrer qu'un nilpotent non nul est un diviseur de zéro.
2. Montrer que si $a \in \mathrm{Nil}(A)$ alors $-a \in \mathrm{Nil}(A)$.
3. Montrer que si $a \in \mathrm{Nil}(A)$ alors $1 + a$ et $1 - a$ sont inversibles.
4. On suppose désormais que A est commutatif.
   (a) Montrer, de deux façons différentes, que $\mathrm{Nil}(A)$ est un idéal de A.
   (b) Montrer que $\overline{0}$ est le seul nilpotent de $A/\mathrm{Nil}(A)$.
   (c) Montrer que $\forall u \in A^*$, $\forall a \in \mathrm{Nil}(A)$, $u + a \in A^*$ et $u - a \in A^*$.
   (d) Montrer que $\mathrm{Nil}(A)$ est l'intersection des idéaux premiers de A.

Exercice 38.
Soit A un anneau commutatif.

1. Soit $f \in A[X] \setminus \{0\}$. Montrer que f est un diviseur de zéro de $A[X]$ si et seulement s'il existe $d \in A \setminus \{0\}$ tel que $df = 0$.
2. Soit $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in A[X]$.
   (a) Montrer que $f \in \mathrm{Nil}(A[X])$ si et seulement si $a_0, a_1, \ldots, a_n \in \mathrm{Nil}(A)$.
   (b) Montrer que $f \in (A[X])^*$ si et seulement si $a_0 \in A^*$ et $a_1, \ldots, a_n \in \mathrm{Nil}(A)$.
   Pour les deux questions précédentes, on pourra utiliser l'exercice précédent.
3. (a) Montrer que si A est intègre alors $(A[X])^* = A^*$ et $\mathrm{Nil}(A[X]) = \{0\}$.
   (b) Le résultat précédent est-il vrai pour un anneau commutatif non trivial quelconque ?

Exercice 39.
Montrer que si A est un anneau commutatif alors $A \setminus A^*$ est la réunion des idéaux maximaux de A.

Exercice 40.
Soit A un anneau commutatif non trivial.
Montrer que les conditions suivantes sont équivalentes :

(i) A possède un unique idéal maximal $\mathfrak{m}$,
(ii) $A \setminus A^*$ est un idéal,
(iii) $\forall a \in A$, $a \in A^*$ ou $1 - a \in A^*$,
(iv) il existe un idéal maximal I tel que $\forall a \in I$, $1 - a \in A^*$.

On dit alors que A est un *anneau local* et que $A/\mathfrak{m}$ est le *corps résiduel* de A.

Exercice 41.

1. Montrer que les idéaux $(X - 1)$ et $(X^2 + X + 1)$ sont comaximaux dans $\mathbb{Q}[X]$.
2. On considère maintenant l'anneau $\mathbb{Z}[X]$.
   (a) Montrer que $\begin{array}{ccc} \mathbb{Z}[X] & \mapsto & \mathbb{Z}/3\mathbb{Z} \\ P & \mapsto & \overline{P(1)} \end{array}$ induit un isomorphisme $\mathbb{Z}[X]/(X - 1, 3) \to \mathbb{Z}/3\mathbb{Z}$.
   (b) Montrer que $(X - 1, 3) = (X - 1, X^2 + X + 1)$.
   (c) Les idéaux $(X - 1)$ et $(X^2 + X + 1)$ sont-ils comaximaux ?
   (d) Montrer que le morphisme canonique $\mathbb{Z}[X] \to \mathbb{Z}[X]/(X-1) \times \mathbb{Z}[X]/(X^2+X+1)$ n'est pas surjectif.

Exercice 42.
Soient $(A, 0, 1, +, \cdot)$ un anneau commutatif et $a, b \in A$.
Montrer que a et b sont étrangers si et seulement si $\overline{a} \in (A/(b))^*$.

Exercice 43.
Pour chacun des morphismes canoniques suivants, montrer qu'il s'agit d'un isomorphisme et déterminer sa réciproque.

1. $\mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$
2. $\mathbb{R}[X]/(X^4 + X^2) \to \mathbb{R}[X]/(X^2) \times \mathbb{R}[X]/(X^2 + 1)$

3 Divisibilité dans les anneaux

Exercice 44.

1. (a) Montrer que $\mathbb{Z}[X]/(2) \simeq (\mathbb{Z}/2\mathbb{Z})[X]$.
   (b) En déduire que $(\mathbb{Z}[X]/(2))^* = \{\overline{1}\}$.
2. On considère $A \coloneqq \mathbb{Z}[X]/(2(X^2-1))$.
   (a) Montrer que les inversibles de A sont $\overline{1}$ et $\overline{-1}$.
   (b) Montrer que $\overline{2}$ et $\overline{2X}$ sont associés.
   (c) Montrer qu'il n'existe pas $u \in A^*$ tel que $\overline{2X} = \overline{2}u$.
   (d) Y a-t-il une contradiction avec le résultat du cours stipulant que deux éléments sont associés si et seulement s'ils sont multiples l'un de l'autre par un inversible ?

Exercice 45.

Soit A un anneau intègre.

1. Montrer que si $a, b \in A$ ont un ppcm alors ils ont un pgcd.
2. La réciproque est-elle vraie ? *On pourra considérer* 2 *et* $1 + i\sqrt{3}$ *dans* $\mathbb{Z}\left[i\sqrt{3}\right]$.

Exercice 46.

Soit A un anneau commutatif.

1. Montrer que si $\pi \in A$ est irréductible et si $u \in A^*$ est inversible alors $u\pi$ est irréductible.
2. Soient $\pi, \pi' \in A$ deux éléments associés de A.
   Montrer que π est irréductible si et seulement si π' l'est.
   Attention : l'anneau A n'est pas supposé intègre.

Exercice 47.

Soient $A \coloneqq \mathbb{Z}[i]$ et $N : A \to \mathbb{N}$ défini par $N(z) \coloneqq |z|^2$.

1. Expliciter $\{z \in A \ : \ N(z) \leq 10\}$.
2. (a) Montrer que $\forall z, w \in A,\ z|w \implies N(z)|N(w)$.
   (b) Étudier la réciproque.
3. (a) Montrer que $\forall z \in A,\ z \in A^* \Leftrightarrow N(z) = 1$.
   (b) En déduire que $A^* = \{\pm 1, \pm i\}$.
4. Les éléments 2 et 3 sont-ils des irréductibles de A ?
5. (a) Soit $z \in A$. Montrer que si $N(z)$ est un nombre premier alors z est un irréductible.
   (b) Étudier la réciproque.
6. Les éléments $2 + i$ et $2 - i$ sont-ils des irréductibles de A ?
7. Lister les éléments $z \in A$ irréductibles vérifiant $N(z) \leq 10$.
8. (a) Décomposer 10, $1 + 5i$, $6 + 8i$ et $-13 + 9i$ en produit de facteurs irréductibles.
   (b) En déduire un pgcd et un ppcm de $1 + 5i$ et $6 + 8i$.

Exercice 48.

1. Montrer que $\mathbb{Z}/6\mathbb{Z}$ est un anneau noethérien non intègre n'admettant pas d'irréductible.
2. Montrer que $\left(\overline{2}\right)$ est un idéal premier de $\mathbb{Z}/6\mathbb{Z}$.
3. Y a-t-il une contradiction avec le résultat du cours énonçant que si (π) est premier non nul alors π est irréductible ?
4. Montrer qu'aucun élément non nul et non inversible de $\mathbb{Z}/6\mathbb{Z}$ s'écrit comme le produit d'un inversible et d'irréductibles.

Exercice 49.

Soit A un anneau commutatif non trivial. On suppose qu'il existe $N : A \to \mathbb{N}$ vérifiant :

(i) $\forall a \in A,\ N(a) = 0 \Leftrightarrow a = 0$
(ii) $\forall a \in A,\ N(a) = 1 \Leftrightarrow a \in A^*$
(iii) $\forall a, b \in A,\ N(ab) = N(a)N(b)$

1. Montrer par récurrence sur $N(a)$ que tout élément $a \in A \setminus \{0\}$ s'écrit de la forme $a = u\pi_1 \cdots \pi_n$ où $u \in A^*$ et où les π_k sont irréductibles.
2. Cette écriture est-elle nécessairement unique ?

Exercice 50.
On considère l'anneau $\mathbb{Z}\left[i\sqrt{3}\right]$.

1. Montrer que 2 est irréductible.
2. Montrer que (2) n'est pas premier.
3. L'anneau $\mathbb{Z}\left[i\sqrt{3}\right]$ est-il factoriel ?

Exercice 51.
On considère $A \coloneqq \{P \in \mathbb{Q}[X] \ : \ P(0) \in \mathbb{Z}\}$.

1. Montrer que A est un anneau intègre pour les lois usuelles.
2. Montrer que $A^* = \{\pm 1\}$, i.e. que les inversibles de A sont 1 et -1.
3. (a) Soit $P \in A$ tel que $P(0) = 0$. Montrer que $\forall m \in \mathbb{Z} \setminus \{0\}$, $m|P$.
   (b) Montrer que les irréductibles de A sont :
   - $\pm p$, où p est un nombre premier ;
   - $\pm P$, où P est un irréductible de $\mathbb{Q}[X]$ tel que $P(0) = 1$.
4. Montrer que X ne s'écrit pas comme produit d'un inversible et d'irréductibles.
5. Est-ce que A est factoriel ?
6. Est-ce que A est noethérien ?
7. Montrer que l'idéal $\left(\frac{X}{2^n},\ n \in \mathbb{N} \setminus \{0\}\right)$ n'est pas principal.

Exercice 52. Soit $A \coloneqq \{P \in \mathbb{Q}[X] \ : \ P'(0) = 0\}$.

1. Montrer que A est un anneau intègre contenant X^2 et X^3.
2. Déterminer A^*.
3. A-t-on $X^2|X^3$ dans A ?
4. Montrer que X^2 et X^3 sont irréductibles et non associés dans A.
5. Exhiber un élément de A admettant deux décompositions distinctes en facteurs irréductibles.
6. L'ideal (X^2) de A est-il premier ?
7. Montrer que l'idéal $I \coloneqq (X^2, X^3)$ de A n'est pas principal.
8. Montrer que les diviseurs unitaires communs à X^5 et X^6 dans A sont 1, X^2 et X^3.
9. En déduire que X^5 et X^6 n'ont pas de pgcd.
10. Justifier de 4 façons différentes que A n'est pas un anneau principal.
11. Montrer que tout élément $P \in A$ s'écrit sous la forme $P = a_0 + a_3X^3 + X^2Q$ où $Q \in A$ et $a_0, a_3 \in \mathbb{Q}$.
12. Identifier l'anneau A/I avec un anneau plus simple.
13. I est-il un idéal maximal de A ?

Exercice 53.

1. Montrer que $\mathbb{Z}[i]$ est un anneau euclidien pour le stathme $\nu(z) \coloneqq |z|^2$.
2. Montrer que $\mathbb{Z}\left[\sqrt{2}\right]$ est un anneau euclidien pour le stathme $\nu\left(a + b\sqrt{2}\right) \coloneqq \left|a^2 - 2b^2\right|$.

Exercice 54. Soit A un anneau. Montrer que les propriétés suivantes sont équivalentes :
(i) A est un corps, (ii) $A[X]$ est euclidien, (iii) $A[X]$ est principal.

Exercice 55. On se place dans l'anneau $\mathbb{R}[X]$.

1. Pour chacun des couples suivants, déterminer un pgcd, un ppcm et une relation de Bézout.
   (a) $X^3 + X + 4$ et $X^2 + X + 2$
   (b) $X^4 + 2X^2 - X + 5$ et $X^4 + 3X^2 + X + 1$
   (c) $X^5 + 2X^3 + X^2 + X + 1$ et $X^4 - 1$
2. Les anneaux suivants sont-ils des corps ? Si oui, les identifier à un corps plus simple.
   (a) $\mathbb{R}[X]/(X^3 + X + 4)$ (b) $\mathbb{R}[X]/(X^2 + X + 2)$

Exercice 56. Soit A un *anneau de Bézout*, i.e. un anneau intègre où tout idéal finiment engendré est principal.

1. Montrer que deux éléments quelconques de A ont un pgcd.
2. Montrer que les propriétés suivantes sont équivalentes :
   (i) A est noethérien, (ii) A est un anneau principal, (iii) A est factoriel.

Exercice 57. L'objectif de cet exercice est de résoudre l'équation diophantienne suivante

(E) $x^3 - y^2 = 2, \quad x, y \in \mathbb{Z}.$

1. Déterminer les inversibles de A.
2. Justifier rapidement que A est factoriel.

On considère (x, y) une solution de (E) et on pose $z := y + i\sqrt{2}$ de sorte que $x^3 = z\bar{z}$ dans A.

3. Montrer que x et y sont impairs.
4. Montrer que z et $\bar{z}$ sont premiers entre eux dans A.
5. En déduire qu'il existe $w \in A$ tel que $z = w^3$ dans A.
6. Conclure : déterminer les solutions de (E).

Exercice 58 (Somme de deux carrés)**.**
Soient $A := \mathbb{Z}[i]$ et $N : A \to \mathbb{N}$ défini par $N(z) := |z|^2$.

1. (a) Montrer que $\forall z \in A,\ z \in A^* \Leftrightarrow N(z) = 1$.
   (b) En déduire que $A^* = \{\pm 1, \pm i\}$.
2. On considère $\Sigma := \left\{n \in \mathbb{N} \ : \ \exists a, b \in \mathbb{N},\ n = a^2 + b^2\right\}$ l'ensemble des entiers qui s'écrivent comme la somme de deux carrés d'entiers.
   (a) Montrer que si $n, m \in \Sigma$ alors $nm \in \Sigma$.
   (b) Soit p un nombre premier.
      i. Montrer que $p \in \Sigma$ si et seulement si p n'est pas un irréductible de A.
      ii. Montrer que $A/(p) \simeq \mathbb{Z}[X]/(X^2 + 1, p) \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(X^2 + \overline{1})$.
      iii. En déduire que p n'est pas irréductible dans A si et seulement si -1 est un carré modulo p si et seulement si $p = 2$ ou $p \equiv 1 \mod 4$.
   (c) Soit $n \in \mathbb{N} \setminus \{0, 1\}$. Montrer que $n \in \Sigma$ ssi $v_p(n)$ est pair pour tout premier $p \equiv 3 \mod 4$.

Exercice 59.

(I) Première partie : quelques propriétés des idempotents.
On rappelle qu'un élément $x \in A$ d'un anneau A est appelé *idempotent* si $x^2 = x$.

(1) Quels sont les idempotents d'un anneau intègre ?
(2) Soit A un anneau. Montrer que si $a \in A$ est idempotent alors $1 - a$ l'est aussi.

Dans la suite de cette partie, on fixe A un anneau *commutatif* et $a, b \in A$ deux idempotents.

(3) (a) Montrer que $a + b - ab$ est idempotent.
   (b) Montrer que $(a, b) = (a + b - ab)$.
(4) (a) Montrer que $b|a$ si et seulement si $a = ab$.
   (b) En déduire que $(a) = (b)$ si et seulement si $a = b$.

(II) Deuxième partie : anneaux absolument plats.
On dit qu'un anneau A est *absolument plat* s'il est commutatif et si $\forall a \in A,\ a \in \left(a^2\right)$.

(5) Montrer qu'un corps est absolument plat.
(6) On suppose dans cette question que A est un anneau absolument plat.
   (a) Soit $a \in A$. Montrer qu'il existe $b \in A$ tel que $a = ba^2$.
   (b) Montrer que, pour a et b comme dans la question précédente, ba est idempotent et $(a) = (ba)$.
   (c) En déduire que tout idéal principal de A est engendré par un idempotent.
(7) Soit A un anneau commutatif. Montrer que A est absolument plat si et seulement si tout idéal finiment engendré de A est engendré par un idempotent.
Indice : on pourra utiliser (6)(c) et (3).

(III) Troisième partie : anneau des idempotents.
Dans cette partie, on considère A un anneau commutatif et $B := \left\{a \in A \ : \ a^2 = a\right\}$.

(8) On définit $\circ : A \times A \to A$ par $a \circ b := a + b - 2ab$.
Montrer que B est stable par $\circ$, i.e. si $a, b \in B$ alors $a \circ b \in B$.
(9) Montrer que $\circ$ admet un neutre dans B, que l'on note e.
(10) Montrer que $(B, \circ, \cdot, e, 1)$ est un anneau commutatif.

Exercice 60.

L'objectif de cet exercice est de montrer que $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais n'est pas euclidien.

(I) Première partie.

L'objectif de cette partie est de montrer que si A est un anneau euclidien alors il existe $x \in A \setminus A^*$ tel que la restriction $\pi_{|A^*\cup\{0\}} : A^* \cup \{0\} \to A/(x)$ de la projection canonique (qui à $y \in A^* \cup \{0\}$ associe $\overline{y}$ la classe de y modulo l'idéal (x)) est surjective.

(1) Montrer que si A est un corps alors un tel x existe.

(2) On suppose maintenant que A est un anneau euclidien qui n'est pas un corps et dont le stathme est noté ν.

(a) Justifier qu'il existe $x \in A$ non nul et non inversible tel que $\nu(x)$ soit minimal.

(b) Montrer qu'un tel x convient.

(3) Déterminer un tel x pour les anneaux euclidiens suivants :

1. $(\mathbb{R}, \nu := 1)$ 2. $(\mathbb{Z}, \nu := |\cdot|)$ 3. $(\mathbb{R}[X], \nu := \deg)$ 4. $\left(\mathbb{Z}[i], \nu := |\cdot|^2\right)$

(II) Deuxième partie.

On pose $\alpha := \dfrac{1+i\sqrt{19}}{2}$ et on considère $A := \mathbb{Z}[\alpha] = \{a + b\alpha \in \mathbb{C} \ : \ a, b \in \mathbb{Z}\}$.

(1) Calculer $\alpha + \overline{\alpha}$ et $\alpha\overline{\alpha}$ et en déduire que α est racine d'un polynôme unitaire à coefficients entiers de degré 2 que l'on exhibera.

(2) Pour $z \in A$, on pose $N(z) := z\overline{z}$.

(a) Montrer que $\forall a, b \in \mathbb{Z},\ N(a + b\alpha) = a^2 + ab + 5b^2$.

(b) Montrer que $\forall z \in A,\ z \in A^* \Leftrightarrow N(z) = 1$.

(c) En déduire que A^* possède deux éléments.

(3) Conclure des questions des deux parties précédentes que A n'est pas euclidien.
Indice : on rappelle que $\mathbb{Z}/2\mathbb{Z}$ est l'unique anneau à deux éléments et que $\mathbb{Z}/3\mathbb{Z}$ est l'unique anneau à trois éléments, à isomorphisme près.

(III) Troisième partie.

(1) Soient $a, b \in A \setminus \{0\}$. Montrer qu'il existe $q, r \in A$ tels que

- $r = 0$ ou $N(r) < N(b)$.
- $a = bq + r$ ou $2a = bq + r$.

Indice : on pourra écrire $\frac{a}{b} = u + v\alpha \in \mathbb{C}$ avec $u, v \in \mathbb{Q}$ et considérer deux cas : $v \notin \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$ et $v \in \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$ où $n = \lfloor v \rfloor$ est la partie entière de v.

(2) (a) Montrer que $A \simeq \mathbb{Z}[X]/(X^2 - X + 5)$.

(b) En déduire que $A/(2)$ est un corps, i.e. que (2) est un idéal maximal de A.

(3) Montrer que A est un anneau principal.
Indice : on pourra adapter la démonstration de la proposition stipulant qu'un anneau euclidien est principal en remplaçant la division euclidienne par le résultat de la question (1) et avec une disjonction de cas.

Exercice 61. Quel est le point commun entre un Nazgûl et un schéma affine ?