Université d'Angers

Théorie des anneaux

Jean-Baptiste Campesato

Version du 14 mai 2025

Table des matières

1 Généralités sur les anneaux

1.1 Anneaux

Définition 1.1. Un *anneau* est la donnée d'un ensemble A contenant deux éléments 0 et 1 non nécessairement distincts et de deux lois de composition internes $+ : A \times A \to A$ et $\cdot : A \times A \to A$ tels que

(1) $(A, 0, +)$ est un groupe abélien :
  (a) $+$ est associative : $\forall a, b, c \in A,\ (a + b) + c = a + (b + c)$
  (b) $+$ est commutative : $\forall a, b \in A,\ a + b = b + a$
  (c) 0 est le neutre de $+$: $\forall a \in A,\ a + 0 = a$
  (d) Tout élément admet un inverse additif : $\forall a \in A,\ \exists b \in A,\ a + b = 0$
(2) $\cdot$ est associative : $\forall a, b, c \in A,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$
(3) 1 est le neutre de $\cdot$: $\forall a \in A,\ 1 \cdot a = a \cdot 1 = a$
(4) $\cdot$ est distributive par rapport à $+$:
  (a) $\forall a, b, c \in A,\ a \cdot (b + c) = a \cdot b + a \cdot c$
  (b) $\forall a, b, c \in A,\ (a + b) \cdot c = a \cdot c + b \cdot c$

Remarque 1.2. Pour des raisons de concision, lorsqu'il n'y a pas de confusion possible, on parlera de l'anneau A plutôt que de l'anneau $(A, 0, 1, +, \cdot)$.

Exemples 1.3.

- $\{0\}$ est l'anneau *trivial* : c'est, à isomorphisme près (notion que l'on définie dans la suite), l'unique anneau à un élément (on dit donc d'un tel anneau qu'il est *trivial*).
- Les ensembles suivants sont des anneaux pour les lois usuelles : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $M_n(\mathbb{R})$, $\mathbb{R}[X]$, $\mathbb{Z}/n\mathbb{Z}$.
- Si $\left(A, 0_A, 1_A, +_A, \cdot_A\right)$ et $\left(B, 0_B, 1_B, +_B, \cdot_B\right)$ sont deux anneaux, alors $(A \times B, 0, 1, +, \cdot)$ est un anneau, appelé *anneau produit*, pour $0 \coloneqq (0_A, 0_B)$, $1 \coloneqq (1_A, 1_B)$, $(a_1, b_1) + (a_2, b_2) \coloneqq (a_1 +_A a_2, b_1 +_B b_2)$ et $(a_1, b_1) \cdot (a_2, b_2) \coloneqq (a_1 \cdot_A a_2, b_1 \cdot_B b_2)$.
- Si $(A, 0, 1, +, \cdot)$ est un anneau alors $A[X]$, l'ensemble des polynômes à coefficients dans A, est un anneau pour les lois usuelles, voir l'Exercice 1.8.
- Si X est un ensemble et si $\left(A, 0_A, 1_A, +_A, \cdot_A\right)$ est un anneau alors $(A^X, 0, 1, +, \cdot)$ est un anneau, où A^X est l'ensemble des fonctions $X \to A$, pour 0 la fonction identiquement égale à 0_A, 1 la fonction identiquement égale à 1_A et les lois $+$ et $\cdot$ définies ponctuellement par $+_A$ et $\cdot_A$ (i.e. pour tout $f, g \in A^X$ et $x \in X$, $(f + g)(x) = f(x) +_A g(x)$ et $(f \cdot g)(x) = f(x) \cdot_A g(x)$).
  Si $X = \varnothing$ alors $A^X = \{\varnothing \to A\}$ est trivial.

Remarque 1.4. On note généralement ab pour $a \cdot b$.

Définition 1.5. On dit qu'un anneau $(A, 0, 1, +, \cdot)$ est *commutatif* s'il vérifie $\forall a, b \in A,\ ab = ba$.

Remarque 1.6. Un anneau est non vide puisqu'il contient un neutre additif.

Proposition 1.7. *Étant donné un anneau $(A, 0, 1, +, \cdot)$, 0 est l'unique neutre additif et 1 est l'unique neutre multiplicatif.*

Démonstration. On ne traite que le cas de 1 puisque la démonstration est similaire pour 0.
Supposons qu'il existe un autre neutre multiplicatif $e \in A$, i.e. vérifiant $\forall a \in A,\ ae = ea = a$, alors

$$\begin{aligned} 1 &= 1 \cdot e && \text{puisque } e \text{ est neutre de } \cdot \\ &= e && \text{puisque 1 est neutre de } \cdot. \end{aligned}$$

■

Proposition 1.8. *L'inverse additif d'un élément d'un anneau est unique.*

Démonstration. Soient $(A,0,1,+,\cdot)$ et $a \in A$. Soient $b,c \in A$ deux inverses additifs de a, i.e. vérifiant $a+b=0$ et $a+c=0$. Alors $c = c+0 = c+a+b = 0+b = b$. ■

Remarque 1.9. Étant donnés $(A,0,1,+,\cdot)$ un anneau et $a \in A$, on note l'inverse additif de a par $-a$. Pour $a,b \in A$, on note $a-b \coloneqq a+(-b)$.

Proposition 1.10. *Soit $(A,0,1,+,\cdot)$ un anneau, alors*
(1) $\forall a \in A,\ a \cdot 0 = 0 \cdot a = 0$
(2) $\forall a,b \in A,\ a(-b) = (-a)b = -(ab)$
(3) $\forall a \in A,\ (-1)a = a(-1) = -a$
(4) $\forall a \in A,\ -(-a) = a$
(5) $\forall a,b \in A,\ (-a)(-b) = ab$
(6) $(-1)(-1) = 1$

Démonstration.

(1) Soit $a \in A$ alors $0 = a\cdot 0 - (a\cdot 0) = a\cdot(0+0) - (a\cdot 0) = a\cdot 0 + a\cdot 0 - (a\cdot 0) = a\cdot 0$.

(2) Soient $a,b \in A$ alors $a(-b) + ab = a(-b+b) = a\cdot 0 = 0$ donc $a(-b) = -(ab)$.
On montre de même que $(-a)b = -(ab)$.

(3) Soit $a \in A$ alors $(-1)a = -(1\cdot a) = -a$ et $a(-1) = -(a\cdot 1) = -a$.

(4) Soit $a \in A$ alors $(-a) + a = 0$ donc $a = -(-a)$ par unicité de l'inverse additif.

(5) Soient $a,b \in A$ alors $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

(6) On a $(-1)(-1) = 1\cdot 1 = 1$. ■

Proposition 1.11. *Un anneau $(A,0,1,+,\cdot)$ est trivial si et seulement si $0=1$.*

Démonstration.

- Supposons que $(A,0,1,+,\cdot)$ soit trivial alors $1 \in A = \{0\}$ donc $0=1$.
- Supposons que $(A,0,1,+,\cdot)$ soit un anneau vérifiant $0=1$.
Soit $a \in A$ alors $a = a\cdot 1 = a\cdot 0 = 0$, donc $A = \{0\}$. ■

Proposition 1.12 (Formule du binôme de Newton)**.** *Soit $(A,0,1,+,\cdot)$ un anneau.*
Si $a,b \in A$ vérifient $ab = ba$ alors

$$\forall n \in \mathbb{N},\ (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Démonstration. Soient $a,b \in A$ vérifiant $ab = ba$. On démontre le résultat par récurrence sur $n \in \mathbb{N}$.

Initialisation au rang $n=0$: $(a+b)^0 = 1$ et $\displaystyle\sum_{k=0}^{0} \binom{0}{0} a^0 b^{0-k} = 1$.

Hérédité : supposons la propriété vraie pour un certain $n \in \mathbb{N}$, alors

$$\begin{aligned}(a+b)^{n+1} &= (a+b)^n(a+b)\\ &= \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right)(a+b)\\ &= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1}\end{aligned}$$

$$
\begin{aligned}
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= a^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=1}^{n} \binom{n}{k} a^k b^{n+1-k} + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}
\end{aligned}
$$

■

Remarque 1.13. La proposition précédente n'est plus vraie si on ne suppose pas que $ab = ba$.
En effet, dans $M_2(\mathbb{R})$, on a

$$\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right)^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

et

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 + 2 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}.$$

1.2 Sous-anneaux

Définition 1.14. Soit $(A, 0, 1, +, \cdot)$ un anneau. On dit que $B \subset A$ est un *sous-anneau* si
(i) $0 \in B$,
(ii) $1 \in B$,
(iii) B est stable par $+$ et $\cdot$, i.e. $\forall a, b \in B$, $a + b \in B$ et $ab \in B$ et
(iv) $(B, 0, 1, +_B, \cdot_B)$ est un anneau où $+_B, \cdot_B : B \times B \to B$ sont les restrictions de $+$ et $\cdot$ à B.

Proposition 1.15. *Soient $(A, 0, 1, +, \cdot)$ un anneau et $B \subset A$. Alors B est un sous-anneau si et seulement si*
(i) $1 \in B$,
(ii) $\forall a, b \in B$, $a - b \in B$ *et*
(iii) $\forall a, b \in B$, $ab \in B$.

Démonstration.

- Si B est un sous-anneau alors $1 \in B$ par définition et, pour tout $a, b \in B$, on a $a - b \in B$ et $ab \in B$ puisque B est un anneau.
- Supposons que B vérifie $1 \in B$, $\forall a, b \in B$, $a - b \in B$ et $\forall a, b \in B$, $ab \in B$.
  Comme $B \neq \emptyset$ et $\forall a, b \in B$, $a - b \in B$, on a déjà que B est un sous-groupe de $(A, 0, +)$.
  Puisque $\forall a, b \in B$, $ab \in B$, B est stable par $\cdot$ et la restriction $\cdot : B \times B \to B$ admet 1 comme neutre et est bien associative et distributive par rapport à $+ : B \times B \to B$. ■

Exemples 1.16.

- $\mathbb{Z} \subset \mathbb{R}$,
- $M_n(\mathbb{Z}) \subset M_n(\mathbb{Q})$,
- $C^0([0, 1], \mathbb{R}) \subset \mathbb{R}^{[0,1]}$,
- $Z(A) \subset A$ où $Z(A) := \{a \in A : \forall x \in A, ax = xa\}$ est le *centre* de A,
- $\mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}\right\} \subset \mathbb{C}$ et $\mathbb{Q}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} : a, b \in \mathbb{Q}\right\} \subset \mathbb{C}$ où $d \in \mathbb{Z}$ et $\sqrt{d} := i\sqrt{-d}$ si $d < 0$ (voir l'Exercice 1.11).

Proposition 1.17. *Une intersection quelconque de sous-anneaux est un sous-anneau.*

Démonstration. Soient $(A,0,1,+,\cdot)$ un anneau et $\mathscr{F}$ un ensemble quelconque de sous-anneaux de A. Posons $C \coloneqq \bigcap_{B\in\mathscr{F}} B$, alors :

- Pour tout $B \in \mathscr{F}$, $1 \in B$. Donc $1 \in C$.
- Soient $a,b \in C$. Alors, pour tout $B \in \mathscr{F}$, on a $a,b \in B$ et donc $ab, a-b \in B$ puisque B est un sous-anneau. Donc $ab \in C$ et $a-b \in C$.

Donc C est un sous-anneau de A. ■

Proposition 1.18. *Soient $(A,0,1,+,\cdot)$ un anneau et $S \subset A$. Il existe un unique plus petit (pour l'inclusion) sous-anneau de A contenant S.*

Démonstration. L'unicité est évidente : si B et C sont tous les deux le plus petit sous-anneau de A contenant S alors $B \subset C$ (puisque B est le plus petit sous-anneau de A contenant S et C contient S) et $C \subset B$ (puisque C est le plus petit sous-anneau de A contenant S et B contient S), donc $B = C$.
Il reste à montrer l'existence.
D'après la proposition précédente $B \coloneqq \bigcap_{\substack{C\supset S\\ C \text{ sous-anneau de } A}} C$ est un sous-anneau de A contenant S.
Si D est un sous-anneau contenant S alors $B \coloneqq \bigcap_{\substack{C\supset S\\ C \text{ sous-anneau de } A}} C \subset D$.
Donc B est le plus petit sous-anneau de A contenant S. ■

1.3 Morphismes

Définition 1.19. Soient $\left(A,0_A,1_A,+_A,\cdot_A\right)$ et $\left(B,0_B,1_B,+_B,\cdot_B\right)$ deux anneaux. Un *morphisme d'anneaux* est une application $f : A \to B$ vérifiant

(i) $f(1_A) = 1_B$,
(ii) $\forall a,b \in A,\ f(a+_A b) = f(a) +_B f(b)$ et
(iii) $\forall a,b \in A,\ f(a\cdot_A b) = f(a)\cdot_B f(b)$.

Proposition 1.20. *Si $f : A \to B$ est un morphisme d'anneaux alors*

- $f(0_A) = 0_B$,
- $\forall a \in A,\ f(-a) = -f(a)$.

Démonstration.

- $0_B = f(0_A) - f(0_A) = f(0_A + 0_A) - f(0_A) = f(0_A) + f(0_A) - f(0_A) = f(0_A)$.
- Soit $a \in A$ alors $f(a) + f(-a) = f(a-a) = f(0_A) = 0_B$ donc $f(-a) = -f(a)$. ■

Puisqu'un morphisme d'anneaux $f : A \to B$ est un morphisme de groupes, on hérite de la proposition suivante où $\ker(f) \coloneqq f^{-1}\left(\{0_B\}\right)$ est le noyau de f (on verra bientôt qu'il s'agit d'un *idéal* de A, i.e. un sous-groupe distingué de A ayant des propriétés supplémentaires liées à la loi $\cdot$ – Attention, si B est non trivial alors $\ker(f)$ n'est pas un sous-anneau de A).

Proposition 1.21. *Un morphisme d'anneaux $f : A \to B$ est injectif si et seulement si* $\ker(f) = \{0_A\}$.

Démonstration.

- Supposons que f est injectif.
  Puisque $f(0_A) = 0_B$, on a $\{0_A\} \subset \ker(f)$.
  Soit $x \in \ker(f)$ alors $f(x) = 0_B = f(0_A)$ donc $x = 0_A$ par injectivité de f.
  Ainsi $\ker(f) = \{0_A\}$.
- Supposons que $\ker(f) = \{0_A\}$.
  Soient $x,y \in A$ tels que $f(x) = f(y)$ alors $f(x-y) = f(x) - f(y) = 0_B$.
  Donc $x - y \in \ker(f) = \{0_A\}$ d'où $x - y = 0_A$ et $x = y$.
  On a montré que $\forall x,y \in A,\ f(x) = f(y) \implies x = y$, i.e. que f est injectif. ■

Proposition 1.22. *Si $f : A \to B$ est un morphisme d'anneaux bijectif alors $f^{-1} : B \to A$ est un morphisme d'anneaux. On dit alors que f est un* isomorphisme *et que A et B sont* isomorphes.

Démonstration. Soit $f : A \to B$ un morphisme d'anneaux bijectif.
- Puisque $f(1_A) = 1_B$, on a $f^{-1}(1_B) = 1_A$.
- Soient $b_1, b_2 \in B$. Notons $a_1 = f^{-1}(b_1)$ et $a_2 = f^{-1}(b_2)$ alors
  - $f^{-1}(b_1 +_B b_2) = f^{-1}\left(f(a_1) +_B f(a_2)\right) = f^{-1}(f(a_1 +_A a_2)) = a_1 +_A a_2 = f^{-1}(b_1) +_A f^{-1}(b_2)$ et
  - $f^{-1}(b_1 \cdot_B b_2) = f^{-1}\left(f(a_1) \cdot_B f(a_2)\right) = f^{-1}(f(a_1 \cdot_A a_2)) = a_1 \cdot_A a_2 = f^{-1}(b_1) \cdot_A f^{-1}(b_2)$. ■

Exemples 1.23.

- L'inclusion $i : \mathbb{Z} \to \mathbb{R}$ est un morphisme d'anneaux (mais pas un isomorphisme).
- La projection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux (mais pas un isomorphisme si $n \geq 1$).
- La conjugaison $c : \mathbb{C} \to \mathbb{C}$ définie par $c(z) := \overline{z}$ est un isomorphisme d'anneaux.
- Soient X est un ensemble non vide, $x \in X$ et $\left(A, 0_A, 1_A, +_A, \cdot_A\right)$ est un anneau. Alors l'application d'évaluation $\mathrm{ev}_x : A^X \to A$ définie par $\mathrm{ev}_x(f) := f(x)$ est une morphisme d'anneaux (mais pas un isomorphisme si $X \neq \{x\}$).
- Soit $P \in Gl_n(\mathbb{R})$. L'application de conjugaison $c : M_n(\mathbb{R}) \to M_n(\mathbb{R})$ définie par $c(M) := P^{-1}MP$ est un isomorphisme d'anneaux.
- Les applications $f : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{R} \\ x & \mapsto & 0 \end{array}$ et $g : \begin{array}{ccc} \mathbb{Z} & \to & M_2 \\ n & \mapsto & \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} \end{array}$ ne sont pas des morphismes d'anneaux : elles préservent $+$ et $\cdot$ mais pas 1.

Proposition 1.24. *Soit $f : A \to B$ un morphisme d'anneaux.*
- *Si $C \subset A$ est un sous-anneau de A alors $f(C)$ est un sous-anneau de B.*
- *Si $D \subset B$ est un sous-anneau de B alors $f^{-1}(D)$ est un sous-anneau de A.*

Démonstration.

- Soit $C \subset A$ un sous-anneau de A, alors :
  - $1 = f(1) \in f(C)$
  - Soient $a, b \in f(C)$, alors il existe $c, d \in C$ tels que $a = f(c)$ et $b = f(d)$.
    Ainsi $a - b = f(c) - f(d) = f(c - d) \in f(C)$ et $ab = f(c)f(d) = f(cd) \in f(C)$.

  Donc $f(C)$ est un sous-anneau de B.
- Soit $D \subset B$ un sous-anneau de B, alors :
  - $f(1) = 1 \in D$ et donc $1 \in f^{-1}(D)$.
  - Soient $a, b \in f^{-1}(D)$. Alors $f(a - b) = f(a) - f(b) \in D$ et $f(ab) = f(a)f(b) \in D$.
    Donc $a - b, ac \in f^{-1}(D)$.

  Donc $f^{-1}(D)$ est un sous-anneau de A. ■

1.4 Anneaux intègres

Définition 1.25. Soit $(A, 0, 1, +, \cdot)$ un anneau.
On dit que A possède des *diviseurs de zéro* s'il existe $a, b \in A \setminus \{0\}$ tels que $ab = 0$.
Le cas échéant, on dit que a est un *diviseur de zéro à gauche* et que b est un *diviseur de zéro à droite*.

Remarque 1.26. Si A est commutatif alors on parle simplement de diviseur de zéro (sans préciser *à gauche* ou *à droite* puisqu'alors un diviseur de zéro à gauche est un diviseur de zéro à droite et vice versa).

Exemples 1.27.

- $\overline{2}$ et $\overline{3}$ sont des diviseurs de zéro de $\mathbb{Z}/6\mathbb{Z}$ puisque $\overline{2}\cdot\overline{3}=\overline{0}$.
- $(1,0)$ et $(0,1)$ sont des diviseurs de zéro de $\mathbb{C}\times\mathbb{C}$ puisque $(1,0)\cdot(0,1)=(0,0)$.
- $\begin{pmatrix}0&1\\0&0\end{pmatrix}$ et $\begin{pmatrix}0&1\\0&0\end{pmatrix}$ sont respectivement un diviseur de zéro à gauche et un diviseur de zéro à droite de $M_2(\mathbb{R})$ puisque $\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$.

Définition 1.28. Un anneau est *intègre* s'il est non trivial, commutatif et ne possède pas de diviseur de zéro.

Remarque 1.29. Un anneau non trivial et commutatif est intègre s'il vérifie

$$\forall a,b\in A,\ ab=0 \implies a=0 \text{ ou } b=0.$$

Exemples 1.30.

- Les anneaux suivants sont intègres (pour les lois usuelles) : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}[X]$ (en considérant le degré), $\mathbb{Z}/p\mathbb{Z}$ où p est premier, $\mathbb{Z}\left[\sqrt{d}\right]$ où $d\in\mathbb{Z}$.
- Si A est un anneau non trivial alors $A\times A$ n'est pas intègre puisque $(1,0)\cdot(0,1)=(0,0)$.
- $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre puisque $\overline{2}\cdot\overline{2}=\overline{0}$.

Proposition 1.31. *Soient $(A,0,1,+,\cdot)$ un anneau **intègre** et $a,b,c\in A$. Si $a\neq 0$ et $ab=ac$ alors $b=c$.*

Démonstration. Soient $a,b,c\in A$ tels que $a\neq 0$ et $ab=ac$. Alors $a(b-c)=ab-ac=0$.
Puisque $a\neq 0$ et que A est intègre, on obtient que $b-c=0$, i.e. que $b=c$. ■

1.5 Éléments inversibles

Définition 1.32. Soit $(A,0,1,+,\cdot)$ un anneau. On dit que $a\in A$ est *inversible* s'il existe $b\in A$ tel que $ab=ba=1$. On dit alors que b est l'*inverse* de a.
On note A^* l'ensemble des inversibles de A.

Remarque 1.33. Lorsque l'on parle d'*inverse* sans précision, il s'agit d'inverse multiplicatif.

Proposition 1.34.

- *Si A est trivial alors $A^*=A$.*
- *Si A est un anneau non trivial alors $A^*\subset A\setminus\{0\}$.*

Démonstration.

- Si A est trivial alors $A=\{1\}$ et $1\cdot 1=1$, donc $A^*=\{1\}=A$.
- Si A est non trivial alors $0\notin A^*$ puisque $\forall a\in A,\ a\cdot 0=0\neq 1$. ■

Proposition 1.35. *Si a admet un inverse alors cet inverse est unique. On le note alors a^{-1}.*

Démonstration. Soit $a\in A$. Supposons que $b,c\in A$ soient deux inverses de a, i.e. b,c vérifient $ba=ab=ca=ac=1$. Alors $b=b\cdot 1=bac=1\cdot c=c$. ■

Proposition 1.36. *Soit $(A,0,1,+,\cdot)$ un anneau. Alors A^* est stable par $\cdot$ et $(A^*,1,\cdot)$ est un groupe.*
De plus, on a

- $\forall a,b\in A^*,\ (ab)^{-1}=b^{-1}a^{-1}$,
- $\forall a\in A^*,\ \left(a^{-1}\right)^{-1}=a$.

Démonstration.

- $1 \in A^*$ puisque $1 \cdot 1 = 1$.
- Soient $a, b \in A^*$ alors
$$(ab)\left(b^{-1}a^{-1}\right) = abb^{-1}a^{-1} = aa^{-1} = 1$$
et
$$\left(b^{-1}a^{-1}\right)(ab) = b^{-1}a^{-1}ab = b^{-1}b = 1.$$
Ainsi ab est inversible d'inverse $b^{-1}a^{-1}$.
Donc la restriction $\cdot : A^* \times A^* \to A^*$ est bien définie et est associative (comme restriction d'une loi associative).
- Soit $a \in A^*$ alors $a^{-1}a = aa^{-1} = 1$. Donc $a^{-1} \in A^*$ d'inverse $\left(a^{-1}\right)^{-1} = a$.
Ainsi a et a^{-1} sont inverses l'un de l'autre.

On a bien montré que $(A^*, 1, \cdot)$ est un groupe. ■

Exemples 1.37.

- $(\mathbb{Z}/2\mathbb{Z})^* = \left\{\overline{1}\right\}$.
- $(\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \left\{\overline{0}\right\}$ où p est premier.
- $(\mathbb{Z}/n\mathbb{Z})^* = \left\{\overline{k} \ : \ \text{pgcd}(k, n) = 1\right\}$.
- $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.
- $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.
- $\mathbb{Z}^* = \{-1, 1\}$.

Proposition 1.38. *Un morphisme d'anneaux $f : A \to B$ induit par restriction un morphisme de groupes $f : A^* \to B^*$.*

Démonstration. Soit $a \in A^*$ alors il existe $b \in A$ tel que $ab = ba = 1$. Ainsi $f(a)f(b) = f(ab) = f(1) = 1$ et $f(b)f(a) = f(ba) = f(1) = 1$. Donc $f(a) \in B^*$.
On a montré que la restriction $f : A^* \to B^*$ est bien définie.
De plus, c'est un morphisme de groupes puisque $\forall a, b \in A^*,\ f(ab) = f(a)f(b)$. ■

1.6 Anneaux à division & corps

Définition 1.39. Un *anneau à division* est un anneau vérifiant $A^* = A \setminus \{0\}$.

Proposition 1.40. *Un anneau à division est non trivial.*

Démonstration. Montrons la contraposée. Supposons que A soit trivial alors $A^* = A \neq \varnothing = A \setminus \{0\}$.
Donc A n'est pas un anneau à division. ■

Proposition 1.41. *Un anneau à division est un anneau non trivial dont tout élément non nul admet un inverse.*

Démonstration. Si A est un anneau à division alors, d'après la proposition précédente, il est non trivial et tout élément non nul admet un inverse puisque $A^* = A \setminus \{0\}$.
Réciproquement si A est un anneau non trivial dont tout élément non nul admet un inverse alors $A \setminus \{0\} \subset A^*$ et donc $A^* = A \setminus \{0\}$ d'après la Proposition 1.34. Donc A est un anneau à division. ■

Définition 1.42. Un *corps* est un anneau à division commutatif.

Exemples 1.43.

- $\mathbb{R}$, $\mathbb{Q}$ et $\mathbb{C}$ sont des corps.
- $\mathbb{Z}$ et $\mathbb{R}[X]$ ne sont pas des anneaux à division (puisque $\mathbb{Z}^* = \{\pm 1\} \neq \mathbb{Z} \setminus \{0\}$ et $X \notin (\mathbb{R}[X])^*$ en considérant le degré).
- L'anneau $\mathbb{H}$ des quaternions, voir l'Exercice 1.14, est un anneau à division non commutatif (donc qui n'est pas un corps).

Proposition 1.44. *Un corps est intègre.*

Démonstration. Soit K un corps. Alors K est un anneau à division et est donc non trivial. De plus K est commutatif par définition.
Soient $a, b \in K$ tels que $ab = 0$. Si $a \neq 0$ alors a est inversible et $b = 1 \cdot b = a^{-1}ab = a^{-1}0 = 0$.
On a bien montré que $\forall a, b \in K,\ ab = 0 \implies a = 0$ ou $b = 0$. Donc K est intègre. ■

Définition 1.45. Soit $(A, 0, 1, +, \cdot)$ un anneau (resp. un corps). Un *sous-anneau à division* (resp. *sous-corps*) de A est un sous-anneau étant un anneau à division (resp. un corps).

On démontre aisément la proposition suivante :

Proposition 1.46. *Soient $(A, 0, 1, +, \cdot)$ un anneau et $B \subset A$. Alors B est un sous-anneau à division (resp. sous-corps) si et seulement si*
(i) $1 \in B$,
(ii) $\forall a, b \in B,\ a - b \in B$,
(iii) $\forall a, b \in B,\ ab \in B$ *et*
(iv) $\forall a \in B \setminus \{0\},\ a^{-1} \in B$.

Remarque 1.47. Un sous-anneau d'un anneau à division (resp. corps) peut ne pas être un sous-anneau à division (resp. un sous-corps), par exemple $\mathbb{Z} \subset \mathbb{Q}$.

Remarque 1.48. Il faut faire attention avec la nomenclature dans la littérature. Pour certains auteurs francophones, un corps désigne un anneau à division, i.e. pour eux un corps n'est pas nécessairement commutatif (ils parlent par exemple du corps $\mathbb{H}$ des quaternions). Ils utilisent aussi les termes de *corps commutatif* pour désigner un anneau à division commutatif et de *corps gauche* pour désigner un anneau à division non commutatif.
La convention adoptée dans ce cours est de réserver le terme *corps* aux anneaux à division commutatifs (ce qui correspond au terme *field* en anglais et au programme actuel de l'agrégation où tous les corps sont supposés commutatifs).

Exercices

Exercice 1.1. Soit $d \in \mathbb{Z}$. Si $d < 0$, on note $\sqrt{d} := i\sqrt{-d}$.

(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 1.2. 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 1.3.

(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 1.4. 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 1.5.
Soit $(A, +, \cdot, 0, 1)$ un anneau. On définit $\oplus : A \times A \to A$ et $\odot : A \times A \to A$ par

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

(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 1.6.

(1) Déterminer, à isomorphisme près, tous les anneaux à 2 éléments.

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

Exercice 1.7. 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 1.8 (Anneaux de polynômes)**.**
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

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

et

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

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

(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) On pose $X \coloneqq (0, 1, 0, 0, \ldots \ldots)$.
Montrer que pour $(a_n)_{n\in\mathbb{N}} \in A[X]$, on a $(a_n)_{n\in\mathbb{N}} = \sum_{n\geq 0} a_n X^n$.
Remarque : pour $n \in \mathbb{N}$, on identifie $a_n \in A$ avec $(a_n, 0, 0, \ldots) \in A[X]$ via le morphisme injectif ι.

(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 1.9. Les sous-ensembles suivants sont-ils des sous-anneaux de $\mathbb{Z}[X]$?
(1) $\{P \in \mathbb{Z}[X] \ : \ \deg(P) \leq n\}$ où $n \in \mathbb{N}$
(2) $\{P \in \mathbb{Z}[X] \ : \ \deg(P) \equiv 0 \mod 2\} \cup \{0\}$
(3) $\{XQ \ : \ Q \in \mathbb{Z}[X]\}$
(4) $\{P(X^2) \ : \ P \in \mathbb{Z}[X]\}$

Exercice 1.10. 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 1.11.
(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 1.12. 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 1.13. Montrer qu'un anneau intègre fini est un corps.

Exercice 1.14.

(1) Montrer que $\mathbb{H} \coloneqq \left\{ \begin{pmatrix} z_1 & -z_2 \\ z_2 & \overline{z_1} \end{pmatrix} \ : \ z_1, z_2 \in \mathbb{C} \right\} \subset M_2(\mathbb{C})$ est un anneau à division non commutatif. $\mathbb{H}$ *est l'anneau des quaternions.*

(2) Montrer que $X^2 + 1 \in \mathbb{H}[X]$ a une infinité de racines.

Exercice 1.15.

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 1.16. 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 1.17. 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 1.18.

(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^*.

Exercice 1.19 (Corps des fractions d'un anneau intègre)**.**
Soit $(A,+,\cdot,0,1)$ un anneau intègre. On munit $A\times(A\setminus\{0\})$ de la relation binaire $\sim$ définie par

$$(a,b)\sim(c,d)\Leftrightarrow ad-bc=0.$$

(1) Montrer que $\sim$ est une relation d'équivalence.
(2) On définit deux lois de composition interne sur $A\times(A\setminus\{0\})$, notées aussi + et $\cdot$, par

$$(a,b)+(c,d):=(ad+bc,bd)\qquad\text{et}\qquad(a,b)\cdot(c,d):=(ac,bd).$$

(a) Justifier que ces deux lois sont bien définies.
(b) Montrer que ces lois sont compatibles avec la relation d'équivalence considérée ci-dessus : i.e. pour $(a_1,b_1),(a_2,b_2),(c_1,d_1),(c_2,d_2)\in A\times(A\setminus\{0\})$,

$$\text{si }\begin{cases}(a_1,b_1)\sim(a_2,b_2)\\(c_1,d_1)\sim(c_2,d_2)\end{cases}\quad\text{alors }\begin{cases}(a_1,b_1)+(c_1,d_1)\sim(a_2,b_2)+(c_2,d_2)\\(a_1,b_1)\cdot(c_1,d_1)\sim(a_2,b_2)\cdot(c_2,d_2)\end{cases}$$

(3) On note $K:=A\times(A\setminus\{0\})/\sim$ l'ensemble des classes d'équivalence de la relation $\sim$ et $\frac{a}{b}:=\overline{(a,b)}\in K$ la classe d'équivalence de $(a,b)\in A\times(A\setminus\{0\})$. On définit $0_K:=\frac{0}{1}$ et $1_K:=\frac{1}{1}$.
On a montré que les lois de la question (2) induisent des lois $+_K$ et $\cdot_K$ sur K vérifiant

$$\frac{a}{b}+_K\frac{c}{d}=\frac{ad+bc}{bd}\qquad\text{et}\qquad\frac{a}{b}\cdot_K\frac{c}{d}=\frac{ac}{bd}.$$

(a) Montrer que $\forall a\in A,\ \forall b,c\in A\setminus\{0\},\ \frac{ac}{bc}=\frac{a}{b}$.
(b) Montrer que $(K,+_K,\cdot_K,0_K,1_K)$ est un corps.
(4) Montrer que $\iota:\begin{array}{ccc}A&\to&K\\a&\mapsto&\frac{a}{1}\end{array}$ est un morphisme d'anneaux injectif.
(5) Soient L un corps et $\varphi:A\to L$ un morphisme d'anneaux injectif.
On définit $\tilde\varphi:K\to L$ par $\tilde\varphi\left(\frac{a}{b}\right):=\varphi(a)\varphi(b)^{-1}$.
(a) Justifier que $\tilde\varphi$ est bien défini.
(b) Montrer que $\tilde\varphi$ est un morphisme d'anneaux injectif.
(c) Montrer que $\tilde\varphi$ est l'unique morphisme d'anneaux $K\to L$ vérifiant $\varphi=\tilde\varphi\circ\iota$.

Le corps K ainsi construit s'appelle le corps des fractions de A *: d'après la question précédente, c'est le plus petit corps contenant A (à isomorphisme près).*

(6) Déterminer le corps des fractions de $\mathbb{Z}$.

2 Idéaux & passage au quotient

2.1 Idéaux

Définition 2.1. Soit $(A,0,1,+,\cdot)$ un anneau. Un *idéal* de A est une partie I vérifiant :
(i) $(I,0,+)$ est un sous-groupe de $(A,0,+)$ et
(ii) $\forall a\in A$, $\forall x\in I$, $ax\in I$ et $xa\in I$.

Remarque 2.2. Certains auteurs considèrent les idéaux à gauche (sous-groupes stables par multiplication à gauche par tout élément de l'anneau), à droite (sous-groupes stables par multiplication à droite par tout élément de l'anneau) et bilatères (idéaux à gauche et à droite). Dans ce cours, on ne considère que des idéaux bilatères (et on utilise simplement le terme *idéal*).

Exemples 2.3. Les parties suivantes des anneaux considérés sont des idéaux :

- $\{0\}\subset A$ où A est un anneau,
- $A\subset A$ où A est un anneau,
- $\ker(f)\subset A$ où $f:A\to B$ est un morphisme d'anneaux,
- $n\mathbb{Z}:=\{nk\ :\ k\in\mathbb{Z}\}\subset\mathbb{Z}$ où $n\in\mathbb{Z}$.

Proposition 2.4. *Soit $(A,0,1,+,\cdot)$ un anneau. Une partie $I\subset A$ est un idéal si et seulement si*
(i) $I\neq\varnothing$ *et*
(ii) $\forall x,y\in I$, $\forall a_1,a_2\in A$, $a_1xa_2+y\in I$.

Démonstration. Supposons que $I\subset A$ soit un idéal. Alors $I\neq\varnothing$ puisque $0\in I$.
Soient $x,y\in I$ et $a_1,a_2\in A$. Alors $a_1x\in I$ et puis $a_1xa_2\in I$ par définition d'un idéal.
Donc $a_1xa_2+y\in I$ puisque $(I,0,+)$ est un sous-groupe de $(A,0,+)$.

Réciproquement, supposons que $I\subset A$ vérifie $I\neq\varnothing$ et $\forall x,y\in I$, $\forall a_1,a_2\in A$, $a_1xa_2+y\in I$.
Alors $I\neq\varnothing$ et $\forall x,y\in I$, $x-y=x+(-1)\cdot y\cdot 1\in I$. Donc $(I,0,+)$ est un sous-groupe de $(A,0,+)$.
Soient $a\in A$ et $x\in I$ alors $ax=ax1+0\in I$ et $xa=1xa+0\in I$.
Donc I est un idéal. ∎

Lorsque A est commutatif, on a la caractérisation légèrement plus simple suivante :

Proposition 2.5. *Soit $(A,0,1,+,\cdot)$ un anneau commutatif. Une partie $I\subset A$ est un idéal si et seulement si*
(i) $I\neq\varnothing$ *et*
(ii) $\forall x,y\in I$, $\forall a\in A$, $ax+y\in I$.

Proposition 2.6. *Soit $f:A\to B$ un morphisme d'anneaux. Si $I\subset B$ est un idéal de B alors $f^{-1}(I)$ est un idéal de A.*

Démonstration.

- $f(0_A)=0_B\in I$ donc $0_A\in f^{-1}(I)$ et $f^{-1}(I)\neq\varnothing$.
- Soient $x,y\in f^{-1}(I)$ et $a_1,a_2\in A$ alors $f(a_1xa_2+y)=f(a_1)f(x)f(a_2)+f(y)\in I$ puisque $f(x),f(y)\in I$ et I est un idéal. Donc $a_1xa_2+y\in f^{-1}(I)$. ∎

Corollaire 2.7. *Soit $f:A\to B$ un morphisme d'anneaux. Alors* $\ker(f):=f^{-1}(\{0\})$ *est un idéal de A.*

Remarque 2.8. L'image d'un idéal par un morphisme d'anneaux n'est généralement pas un idéal. En effet, si on considère l'inclusion $\imath:\mathbb{Z}\to\mathbb{Q}$ alors $\imath(\mathbb{Z})=\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$.

Proposition 2.9. *Une intersection quelconque d'idéaux est un idéal.*

Démonstration. Soient $(A,0,1,+,\cdot)$ un anneau et $\mathscr{F}$ un ensemble quelconque d'idéaux de A.
Posons $I \coloneqq \bigcap_{J\in\mathscr{F}} J$, alors :

- Pour tout $J \in \mathscr{F}$, $0 \in J$. Donc $0 \in I$ et $I \neq \varnothing$.
- Soient $x, y \in I$ et $a_1, a_2 \in A$. Alors, pour tout $J \in \mathscr{F}$, on a $a_1 x a_2 + y \in J$ puisque J est un idéal. Donc $a_1 x a_2 + y \in I$.

Donc I est un idéal de A. ■

Proposition 2.10. *Soient $(A,0,1,+,\cdot)$ un anneau et $S \subset A$. Il existe un unique plus petit (pour l'inclusion) idéal de A contenant S. On note cet idéal (S) et on dit que (S) est l'idéal de A* engendré *par S.*

Démonstration. L'unicité est évidente : si I et J sont tous les deux le plus petit idéal de A contenant S alors $I \subset J$ (puisque I est le plus petit idéal de A contenant S et J contient S) et $J \subset I$ (puisque J est le plus petit idéal de A contenant S et I contient S), donc $I = J$.
Il reste à montrer l'existence.
D'après la proposition précédente $I \coloneqq \bigcap_{\substack{J\supset S \\ J \text{ idéal de } A}} J$ est un idéal de A contenant S.
Si K est un idéal de A contenant S alors $I \coloneqq \bigcap_{\substack{J\supset S \\ J \text{ idéal}}} J \subset K$.
Donc I est le plus petit idéal de A contenant S. ■

Remarque 2.11. Si $a_1,\dots,a_k \in A$, on note $(a_1,\dots,a_k) \coloneqq \big(\{a_1,\dots,a_k\}\big)$ l'idéal de A engendré par $a_1,\dots,a_k$.

Proposition 2.12. *Soient $(A,0,1,+,\cdot)$ un anneau et $S \subset A$ une partie non vide. Alors*

$$(S) = \left\{ \sum_{i=1}^{n} a_i s_i b_i \ : \ n \in \mathbb{N}\setminus\{0\},\ a_i, b_i \in A,\ s_i \in S \right\}.$$

Démonstration. Notons $I \coloneqq \left\{ \sum_{i=1}^{n} a_i s_i b_i \ : \ n \in \mathbb{N}\setminus\{0\},\ a_i, b_i \in A,\ s_i \in S \right\}$.

- I est un idéal :
  - ⋆ Soit $s \in S$ alors $0 = 0 \cdot s \cdot 0 \in I$.
  - ⋆ Soient $x, y \in I$ et $\alpha_1, \beta_1 \in A$.
    Alors il existe $a_1,\dots,a_n,b_1,\dots,b_n,a'_1,\dots,a'_m,b'_1,\dots,b'_m \in A$ et $s_1,\dots,s_n,s'_1,\dots,s'_m \in S$ tels que
    $$x = \sum_{i=1}^{n} a_i s_i b_i \quad \text{et} \quad y = \sum_{j=1}^{m} a'_j s'_j b'_j.$$
    Ainsi
    $$\alpha_1 x \alpha_2 + y = \sum_{i=1}^{n} \alpha_1 a_i s_i b_i \alpha_2 + \sum_{j=1}^{m} a'_j s'_j b'_j \in I.$$
- I contient S : soit $s \in S$ alors $s = 1 \cdot s \cdot 1 \in I$.
- I est le plus petit idéal contenant S :
  Soit J un idéal contenant S. Soit $x \in I$.
  Alors il existe $a_1,\dots,a_n,b_1,\dots,b_n \in A$ et $s_1,\dots,s_n \in S$ tels que $x = \sum_{i=1}^{n} a_i s_i b_i$.
  Puisque J est un idéal et que, $\forall i \in \{1,\dots,n\}$, $s_i \in S \subset J$, on a que $x \in I$.

Donc I est le plus petit idéal contenant S, i.e. $I = (S)$. ■

Remarque 2.13. Si $(A,0,1,+,\cdot)$ est un anneau alors $(\varnothing) = (0) = \{0\}$.

2.2 Anneaux quotients

Proposition 2.14. *Soient $(A,0,1,+,\cdot)$ un anneau et $I \subset A$ un idéal de A. On définit A/I comme l'ensemble des classes d'équivalence de A pour la relation d'équivalence $a \sim b \Leftrightarrow a-b \in I$.*
Alors

$$+_{A/I} : \begin{array}{ccc} (A/I)\times(A/I) & \to & A/I \\ (\overline{a},\overline{b}) & \mapsto & \overline{a+b} \end{array}$$

et

$$\cdot_{A/I} : \begin{array}{ccc} (A/I)\times(A/I) & \to & A/I \\ (\overline{a},\overline{b}) & \mapsto & \overline{a\cdot b} \end{array}$$

sont bien définies et confèrent à A/I une structure d'anneau avec $0_{A/I} := \overline{0}$ et $1_{A/I} := \overline{1}$.
De plus la projection canonique $\pi : A \to A/I$ définie par $\pi(a) = \overline{a}$ est un morphisme d'anneaux.

Démonstration. Puisque I est un sous-groupe d'un groupe commutatif, c'est un sous-groupe distingué et $(A/I, 0_{A/I}, +_{A/I})$ est un groupe. Il reste donc à vérifier que le produit passe au quotient.
Soient $a,b,c,d \in A$ tels que $\overline{a} = \overline{c}$ et $\overline{b} = \overline{d}$ alors $x := a-c \in I$ et $y := b-d \in I$. Donc $ab - cd = (x+c)(y+d) - cd = xy + xd + cy \in I$. Ainsi $\overline{ab} = \overline{cd}$.
On vérifie maintenant aisément que $\left(A/I, 0_{A/I}, 1_{A/I}, +_{A/I}, \cdot_{A/I}\right)$ est un anneau. ■

Exemples 2.15.

- $\mathbb{Z}/n\mathbb{Z}$ est l'anneau quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$ (où $n \in \mathbb{Z}$).
- L'anneau quotient $\mathbb{R}[X]/(X^2+1)$ est isomorphe à $\mathbb{C}$ par l'isomorphisme $a+ib \mapsto \overline{a+bX}$.

Théorème 2.16 (Propriété universelle du quotient)**.** *Soient $f : A \to B$ un morphisme d'anneaux et $I \subset A$ un idéal de A tel que $I \subset \ker(f)$.*
Alors il existe un unique morphisme d'anneaux $\overline{f} : A/I \to B$ tel que $f = \overline{f} \circ \pi$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{f}} & \\ A/I & & \end{array}$$

Démonstration.

- Montrons que l'application $\overline{f} : \begin{array}{ccc} A/I & \to & B \\ \overline{a} & \mapsto & f(a) \end{array}$ est bien définie.
  Soient $a,b \in A$ tels que $\overline{a} = \overline{b}$ alors $a-b \in I \subset \ker(f)$ donc $f(a) - f(b) = f(a-b) = 0$, i.e. $f(a) = f(b)$.
- Montrons que $\overline{f}$ est un morphisme d'anneaux.
  - ⋆ $\overline{f}\left(\overline{1}\right) = f(1) = 1$
  - ⋆ Soient $a,b \in A$ alors $\overline{f}\left(\overline{a}+\overline{b}\right) = \overline{f}\left(\overline{a+b}\right) = f(a+b) = f(a) + f(b) = \overline{f}\left(\overline{a}\right) + \overline{f}\left(\overline{b}\right)$ et $\overline{f}\left(\overline{a}\cdot\overline{b}\right) = \overline{f}\left(\overline{ab}\right) = f(ab) = f(a)\cdot f(b) = \overline{f}\left(\overline{a}\right)\overline{f}\left(\overline{b}\right)$.
- Montrons que $f = \overline{f} \circ \pi$.
  Soit $a \in A$ alors $\overline{f} \circ \pi(a) = \overline{f}\left(\overline{a}\right)$.
- Montrons que $\overline{f}$ est l'unique morphisme d'anneaux $A/I \to B$ vérifiant $f = \overline{f} \circ \pi$.
  Soit $g : A/I \to B$ vérifiant $f = g \circ \pi$. Soit $x \in A$ alors $g\left(\overline{x}\right) = g \circ \pi(x) = f(x) = \overline{f}\left(\overline{x}\right)$. ■

Remarque 2.17. On vérifie aisément que $\mathrm{im}(f) = \mathrm{im}\left(\overline{f}\right)$.

Soit $y \in \mathrm{im}(f)$. Alors il existe $x \in A$ tel que $y = f(x)$. Ainsi $y = f(x) = \overline{f}(\pi(x)) \in \mathrm{im}\left(\overline{f}\right)$.

Donc $\mathrm{im}(f) \subset \mathrm{im}\left(\overline{f}\right)$.

Montrons l'inclusion réciproque. Soit $y \in \mathrm{im}\left(\overline{f}\right)$ alors il existe $x \in A$ tel que $y = \overline{f}\left(\overline{x}\right)$.

Ainsi $y = \overline{f}\left(\overline{x}\right) = \overline{f}(\pi(x)) = f(x) \in \mathrm{im}(f)$.

Corollaire 2.18. *Soient A, B deux anneaux et $I \subset A$ un idéal de A. Alors*

$$\begin{array}{ccc} \mathrm{Hom}(A/I, B) & \to & \{f \in \mathrm{Hom}(A,B) \ : \ I \subset \ker(f)\} \\ \varphi & \mapsto & \varphi \circ \pi \\ \overline{f} & \leftarrow\!\shortmid & f \end{array}$$

est une bijection.

2.3 Théorèmes d'isomorphisme

Proposition 2.19. *Un morphisme d'anneaux $f : A \to B$ induit un morphisme d'anneaux injectif $\overline{f} : A/\ker(f) \to B$.*

Démonstration. Soit $f : A \to B$ une morphisme d'anneaux. Alors, par propriété universelle du quotient, f induit un unique morphisme d'anneaux $\overline{f} : A/\ker(f) \to B$ vérifiant $f = \overline{f} \circ \pi$ où $\pi : A \to A/\ker(f)$ est la projection canonique. Montrons que $\overline{f}$ est injectif.
Soit $\overline{x} \in \ker\left(\overline{f}\right)$ alors $0 = \overline{f}\left(\overline{x}\right) = \overline{f}(\pi(x))) = f(x)$. Donc $x \in \ker(f)$ et $\overline{x} = \overline{0} \in A/\ker(f)$.
Ainsi $\ker\left(\overline{f}\right) = \left\{\overline{0}\right\}$, i.e. $\overline{f}$ est injectif. ■

Théorème 2.20 (Premier théorème d'isomorphisme)**.**
Un morphisme d'anneaux $f : A \to B$ induit un isomorphisme d'anneaux $\overline{f} : A/\ker(f) \to \mathrm{im}(f)$.

Démonstration. Soit $f : A \to B$ une morphisme d'anneaux. Alors, par propriété universelle du quotient, f induit un unique morphisme d'anneaux $\overline{f} : A/\ker(f) \to B$ vérifiant $f = \overline{f} \circ \pi$ où $\pi : A \to A/\ker(f)$ est la projection canonique. On a vu dans la proposition précédente que $\overline{f}$ est injectif et dans la Remarque 2.17 que $\mathrm{im}\left(\overline{f}\right) = \mathrm{im}(f)$. ■

Théorème 2.21 (Troisième théorème d'isomorphisme)**.**
Soient $(A, 0, 1, +, \cdot)$ un anneau et $I \subset J \subset A$ deux idéaux de A. Notons $\pi_I : A \to A/I$ la projection canonique. Alors $J/I \coloneqq \pi_I(J) = \left\{\overline{x} \in A/I \ : \ x \in J\right\}$ est un idéal de A/I et il y a un isomorphisme $(A/I)/(J/I) \to A/J$.

Démonstration. Notons $\pi_J : A \to A/J$ la projection canonique. C'est un morphisme d'anneaux surjectif et $I \subset J = \ker(\pi_J)$, donc, d'après la propriété universelle du quotient et la Remarque 2.17, π_J induit un morphisme d'anneaux surjectif $\varphi : A/I \to A/J$ vérifiant $\pi_J = \varphi \circ \pi_I$.

Montrons que $\ker(\varphi) = J/I$. Soit $y \in J/I$, alors il existe $x \in J$ tel que $y = \pi_I(x)$, alors $\varphi(y) = \varphi(\pi_I(x)) = \pi_J(x) = 0$. Donc $y \in \ker(\varphi)$.
Réciproquement, soit $y \in \ker(\varphi)$. Il existe $x \in A$ tel que $y = \pi_I(x)$. Et $\overline{0} = \varphi(y) = \varphi(\pi_I(x)) = \pi_J(x)$ donc $x \in \ker(\pi_J) = J$. Ainsi $y = \overline{x} \in J/I$.

Donc $J/I = \ker(\varphi)$ est un idéal de A/I. Et, d'après le premier théorème d'isomorphisme appliqué à φ, il existe un isomorphisme $(A/I)/(J/I) \to A/J$. ■

Le résultat suivant permet de décrire les idéaux de A/I à partir des idéaux de A contenant I.

Corollaire 2.22. *Soient $(A,0,1,+,\cdot)$ un anneau et $I \subset A$ un idéal de A.*
Alors la projection canonique $\pi : A \to A/I$ induit une bijection

$$\begin{array}{ccc} \{\textit{Idéaux de } A \textit{ contenant } I\} & \to & \{\textit{Idéaux de } A/I\} \\ J & \mapsto & J/I \\ \pi^{-1}(J) & \leftarrow\!\shortmid & J \end{array}.$$

Démonstration. L'application $\{\text{Idéaux de } A \text{ contenant } I\} \ni J \mapsto J/I \in \{\text{Idéaux de } A/I\}$ est bien définie d'après le troisième théorème d'isomorphisme. Si J est un idéal de A/I alors $I = \pi^{-1}\left(\overline{0}\right) \subset \pi^{-1}(J)$. Donc l'application $\{\text{Idéaux de } A/I\} \ni J \mapsto \pi^{-1}(J) \in \{\text{Idéaux de } A \text{ contenant } I\}$ est elle aussi bien définie. Vérifions qu'elles sont réciproques l'une de l'autre.

- Soit J un idéal de A contenant I. Alors $\pi^{-1}(J/I) = \pi^{-1}(\pi(J)) \supset J$.
  Réciproquement, soit $x \in \pi^{-1}(J/I)$. Alors $\pi(x) \in J/I = \pi(J)$, donc il existe $y \in J$ tel que $\pi(x) = \pi(y)$. On déduit de $\pi(x-y) = \overline{0}$ que $x - y \in I \subset J$. Donc $x = (x-y) + y \in J$ puisque J est un idéal (donc un sous-groupe).
  Ainsi $\pi^{-1}(J/I) = \pi^{-1}(\pi(J)) = J$.
- Soit J un idéal de A/I alors, puisque π est surjective, $\pi^{-1}(J)/I = \pi\left(\pi^{-1}(J)\right) = J$. ∎

On démontre le résultat suivant dans l'Exercice 2.9.

Théorème 2.23 (Deuxième théorème d'isomorphisme)**.**
Soient $(A,0,1,+,\cdot)$ un anneau, $B \subset A$ un sous-anneau de A et $I \subset A$ un idéal de A.
Alors $B+I$ est un sous-anneau de A, $B \cap I$ est un idéal de B et il y a un isomorphisme $B/(B\cap I) \to (B+I)/I$.

2.4 Idéaux et anneaux principaux

Définition 2.24. Soit $(A,0,1,+,\cdot)$ un anneau. On dit qu'un idéal $I \subset A$ de A est *principal* s'il existe $a \in A$ tel que $I = (a)$.

Définition 2.25. Un anneau *principal* est un anneau intègre dont tous les idéaux sont principaux.

Exemples 2.26. Grâce à la division euclidienne, on vérifie que les anneaux $\mathbb{Z}$ et $\mathbb{R}[X]$ sont principaux (on généralisera cette observation dans la Section 3).

Proposition 2.27. *Soient $(A,0,1,+,\cdot)$ un anneau et $I \subset A$ un idéal de A, alors*
(1) *$I = A \Leftrightarrow I \cap A^* \neq \emptyset$ (i.e. $I = A$ si et seulement si I contient un inversible) ;*
(2) *si A est commutatif alors $\forall a \in A$, $(a) = A \Leftrightarrow a \in A^*$;*
(3) *si A est intègre alors $\forall a, b \in A$, $(a) = (b) \Leftrightarrow \exists u \in A^*$, $b = au$.*

Démonstration.
(1) $\Rightarrow$ Supposons que $I = A$ alors $1 \in I \cap A^*$. Donc $I \cap A^* \neq \emptyset$.
$\Leftarrow$ Supposons que $I \cap A^* \neq \emptyset$ alors il existe $u \in I \cap A^*$.
Soit $a \in A$, alors $a = uu^{-1}a \in I$. Donc $A \subset I$ et ainsi $A = I$.
(2) Supposons que A soit commutatif.
$\Rightarrow$ Soit $a \in A$ tel que $(a) = A$. Alors $1 \in (a)$, donc il existe $u \in A$ tel que $1 = au$. Ainsi $a \in A^*$.
$\Leftarrow$ Soit $a \in A^*$ alors $a \in (a) \cap A^*$. Donc, d'après le premier point, $(a) = A$.
(3) Supposons que A soit intègre.
$\Rightarrow$ Soient $a, b \in A$ tels que $(a) = (b)$. Alors $b \in (b) = (a)$ donc il existe $u \in A$ tel que $b = au$.
De même, il existe $v \in A$ tel que $a = bv$. Ainsi $a = bv = auv$ d'où $a(1-uv) = 0$.
Soit $a = 0$ et alors $b = au = 0$, d'où $a = b \cdot 1$ avec $A \in A^*$.
Soit $a \neq 0$ et alors, puisque A est intègre, $1 = uv$, donc $u \in A^*$ et $b = au$.
$\Leftarrow$ Supposons qu'il existe $u \in A^*$ tel que $b = au$.
Soit $x \in (b)$ alors il existe $\beta \in A$ tel que $x = b\beta = au\beta \in (a)$. Donc $(b) \subset (a)$.
Soit $y \in (a)$ alors il existe $\alpha \in A$ tel que $y = a\alpha = bu^{-1}\alpha \in (b)$. Donc $(a) \subset (b)$.
Ainsi $(a) = (b)$. ∎

Remarque 2.28. Soient A un anneau commutatif et $a, b \in A$.
S'il existe u inversible tel que $a = bu$ alors $(a) = (b)$ sans hypothèse d'intégrité (l'hypothèse n'a pas été utilisée dans la démonstration de cette implication).
En revanche, la réciproque n'est généralement pas vraie si A n'est pas supposé intègre (Exercice 3.1).

2.5 Idéaux premiers et maximaux d'un anneau commutatif

Définition 2.29. Soit $(A, 0, 1, +, \cdot)$ un anneau commutatif. Un idéal $P \subset A$ de A est *premier* si
(i) $P \neq A$, et
(ii) $\forall a, b \in A,\ ab \in P \implies a \in P$ ou $b \in P$.

Exemple 2.30. Si p est premier alors $p\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$.
D'abord, $p\mathbb{Z} \neq \mathbb{Z}$ puisque $1 \notin p\mathbb{Z}$.
Soient $a, b \in \mathbb{Z}$ tels que $ab \in p\mathbb{Z}$ alors $p|ab$.
D'après le lemme d'Euclide, $p|a$ ou $p|b$, i.e. $a \in p\mathbb{Z}$ ou $b \in p\mathbb{Z}$.

Définition 2.31. Soit $(A, 0, 1, +, \cdot)$ un anneau commutatif. Un idéal $\mathfrak{m} \subset A$ de A est *maximal* si
(i) $\mathfrak{m} \neq A$, et
(ii) $\mathfrak{m}$ est maximal dans l'ensemble des idéaux distincts de A,
i.e. pour tout idéal I de A si $\mathfrak{m} \subset I$ alors $I = \mathfrak{m}$ ou $I = A$.

Exemple 2.32. Si p est premier alors $p\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$.
D'abord, $p\mathbb{Z} \neq \mathbb{Z}$ puisque $1 \notin p\mathbb{Z}$.
Soit I un idéal de $\mathbb{Z}$ tel que $p\mathbb{Z} \subset I$. Puisque $\mathbb{Z}$ est principal, il existe $n \in \mathbb{Z}$ tel que $I = n\mathbb{Z}$.
Donc $p \in p\mathbb{Z} \subset I = n\mathbb{Z}$, ainsi $n|p$.
Puisque p est premier alors $n = \pm 1$ et alors $I = \mathbb{Z}$ ou $n = \pm p$ et alors $I = p\mathbb{Z}$.

Théorème 2.33 (Théorème de Krull)**.** *Soient $(A, 0, 1, +, \cdot)$ un anneau commutatif et $I \subsetneq A$ un idéal de A distinct de A. Alors il existe un idéal maximal de A contenant I.*

La démonstration du théorème de Krull repose sur le lemme de Zorn. En fait, le théorème de Krull et le lemme de Zorn sont équivalents. Ils sont aussi équivalents à l'axiome du choix qui stipule que si $(S_i)_{i\in I}$ est une famille d'ensembles non vides alors $\prod_{i\in I} S_i \neq \emptyset$.

Lemme 2.34 (Lemme de Zorn)**.**
Soit $(E, \leq)$ un ensemble ordonné non vide tel que toute partie de E totalement ordonnée possède un majorant. Alors E admet un élément maximal, i.e. $\exists m \in E,\ \forall x \in E,\ m \leq x \implies x = m$.

Démonstration du Théorème de Krull. On considère $E := \{J \subset A \ :\ J \text{ idéal de } A,\ J \neq A,\ I \subset J\}$, alors
- E est ordonné par l'inclusion $\subset$.
- $E \neq \emptyset$ puisque $I \in E$.
- Soit $\mathscr{F}$ une partie de E totalement ordonnée non vide (si $\mathscr{F}$ est vide alors elle est majorée par n'importe quel élément de E). Posons $K := \bigcup_{J\in\mathscr{F}} J$ alors
  - $K \neq \emptyset$ puisque $0 \in I \subset K$.
  - K est un idéal de A. En effet, soient $x_1, x_2 \in K$ et $a \in A$, alors il existe $J_1, J_2 \in \mathscr{F}$ tels que $x_1 \in J_1$ et $x_2 \in J_2$. Puisque $\mathscr{F}$ est totalement ordonnée, soit $J_1 \subset J_2$ et alors on pose $\tilde{J} := J_2$, soit $J_2 \subset J_1$ et alors on pose $\tilde{J} := J_1$.
    Alors, puisque $\tilde{J}$ est un idéal et $x_1, x_2 \in \tilde{J}$, on a $x_1 + ax_2 \in \tilde{J} \subset K$.
  - $K \neq A$. Supposons par l'absurde que $K = A$, alors il existe $J \in \mathscr{F}$ tel que $1 \in J$. Donc $J = A$ d'où une contradiction.

  Donc $K \in E$. De plus K est un majorant de $\mathscr{F}$ puisque pour tout $J \in \mathscr{F}$, $J \subset K$.

On déduit du lemme de Zorn que E admet un élément maximal $\mathfrak{m}$. ■

Corollaire 2.35. *Tout anneau commutatif non trivial admet un idéal maximal.*

Démonstration. Soit $(A, 0, 1, +, \cdot)$ un anneau commutatif non trivial. Alors $\{0\}$ est un idéal de A distinct de A. Donc, d'après le théorème de Krull, il existe un idéal maximal $\mathfrak{m}$ de A tel que $\{0\} \subset \mathfrak{m}$. ■

Remarque 2.36. On peut démontrer que le corollaire est équivalent au théorème de Krull.
En effet, soit $(A,0,1,+,\cdot)$ un anneau commutatif et $I \subsetneq A$ un idéal de A distinct de A. Alors A/I est un anneau commutatif non trivial, donc d'après le corollaire, A/I admet un idéal maximal $\mathfrak{m}$. On vérifie ensuite aisément que $\pi^{-1}(\mathfrak{m})$ est un idéal maximal de A contenant I.
Ainsi, dans certains livres, c'est le corollaire qui est appelé *théorème de Krull*.

Proposition 2.37. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $I \subset A$ un idéal de A, alors*
(1) *I est premier si et seulement si A/I est intègre.*
(2) *I est maximal si et seulement si A/I est un corps.*

Démonstration. Notons déjà que A/I est commutatif puisque A l'est.

(1) $\Rightarrow$ Soit I un idéal premier de A. Alors $I \neq A$ donc $A/I \neq \{\overline{0}\}$.
Soient $a,b \in A$ tels que $\overline{a}\overline{b} = \overline{0}$ alors $\overline{ab} = \overline{a}\overline{b} = \overline{0}$ donc $ab \in I$. Puisque I est premier, soit $a \in I$ et alors $\overline{a} = \overline{0}$, soit $b \in I$ et alors $\overline{b} = \overline{0}$.
Donc A/I est intègre.

$\Leftarrow$ Supposons que A/I soit intègre. Alors A/I n'est pas trivial et donc $I \neq A$.
Soient $a,b \in A$ tels que $ab \in I$ alors $\overline{a}\overline{b} = \overline{ab} = \overline{0}$.
Puisque A/I est intègre, soit $\overline{a} = \overline{0}$ et alors $a \in I$, soit $\overline{b} = \overline{0}$ et $b \in I$.
Donc I est premier.

(2) $\Rightarrow$ Soit I un idéal maximal de A. Alors $I \neq A$ donc $A/I \neq \{\overline{0}\}$.
Soit $x \in (A/I) \setminus \left\{\overline{0}\right\}$ alors il existe $a \in A \setminus I$ tel que $x = \overline{a}$.
Posons $J := (a) + I$. Alors J est un idéal de A vérifiant $I \subsetneq J$ puisque $a \in J \setminus I$.
Par maximalité de I, $J = A$ et donc $1 \in J$. Ainsi, il existe $u \in A$ et $b \in I$ tel que $1 = au + b$.
Enfin $\overline{1} = \overline{au+b} = \overline{a} \cdot \overline{u} + \overline{b} = \overline{a} \cdot \overline{u}$. Donc $x = \overline{a}$ est inversible dans A/I.
Ainsi A/I est un corps.

$\Leftarrow$ Supposons que A/I soit un corps. Alors A/I n'est pas trivial et donc $I \neq A$.
Soit J un idéal de A tel que $I \subsetneq J$.
Alors il existe $a \in J \setminus I$. Donc $\overline{a} \in (A/I) \setminus \left\{\overline{0}\right\} = (A/I)^*$ car A/I est un corps.
Ainsi il existe $b \in A$ tel que $\overline{a} \cdot \overline{b} = \overline{1}$. Donc $\overline{1-ab} = \overline{0}$, i.e. $1 - ab \in I \subset J$.
Puisque J est un idéal, on a $1 = (1-ab) + ab \in J$. Donc $J = A$.
Ainsi I est maximal. ■

Corollaire 2.38. *Un idéal maximal est premier.*

Démonstration. Soit A un anneau commutatif et $\mathfrak{m}$ un idéal maximal.
Alors $A/\mathfrak{m}$ est un corps et est donc intègre. Ainsi $\mathfrak{m}$ est premier. ■

Remarque 2.39. La réciproque est fausse : prenons $A := \mathbb{Z}[X]$ et $I := (X)$ alors $A/I \simeq \mathbb{Z}$ est intègre mais n'est pas un corps. Donc I est un anneau premier qui n'est pas maximal.

2.6 Théorème des restes chinois

Définition 2.40. Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $I,J \subset A$ deux idéaux de A.
On dit que I et J sont *comaximaux* si $I + J = A$.

Proposition 2.41. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $I,J \subset A$ deux idéaux de A.*
Alors I et J sont comaximaux si et seulement si $\exists a \in I$, $\exists b \in J$, $a + b = 1$.

Démonstration.

- Supposons que I et J soient comaximaux. Puisque $1 \in A = I + J$, il existe $a \in I$ et $b \in J$ tels que $1 = a + b$.

- Réciproquement, supposons qu'il existe $a \in I$ et $b \in J$ tels que $1 = a + b$.
  Soit $x \in A$. Alors $x = 1 \cdot x = ax + bx \in I + J$ puisque I et J sont des idéaux.
  Donc $A \subset I + J$ et donc $I + J = A$. ■

Exemples 2.42. Soient $m, n \in \mathbb{Z}$. Alors $m\mathbb{Z}$ et $n\mathbb{Z}$ sont comaximaux si et seulement si $\text{pgcd}(m, n) = 1$.
Supposons que $m\mathbb{Z}$ et $n\mathbb{Z}$ soient comaximaux. Alors, il existe $k, l \in \mathbb{Z}$ tels que $1 = mk + nl$.
Si d est un diviseur commun de m et n alors $d | mk + nl = 1$. Ainsi $\text{pgcd}(m, b) = 1$.
Réciproquement, supposons que $\text{pgcd}(m, n) = 1$.
Alors, d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $1 = mu + nv$.
Soit $x \in \mathbb{Z}$ alors $x = 1 \cdot x = mux + nvx \in m\mathbb{Z} + n\mathbb{Z}$. Donc $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$, i.e. $m\mathbb{Z}$ et $n\mathbb{Z}$ sont comaximaux.

Lemme 2.43. *Soient $(A, 0, 1, +, \cdot)$ un anneau commutatif et $I_1, \dots, I_n, J \subset A$ des idéaux de A.*

Si, pour tout $k \in 1, \dots, n$, I_k et J sont comaximaux alors $\bigcap_{k=1}^{n} I_k$ et J sont comaximaux.

Démonstration. Supposons que pour tout $k \in 1, \dots, n$, I_k et J sont comaximaux.
Pour $k \in \{1, \dots, n\}$, comme I_k et J sont comaximaux,il existe $a_k \in I_k$ et $b_k \in J$ tels que $1 = a_k + b_k$.
Alors $1 = \prod_{k=1}^{n}(a_k + b_k) = \prod_{k=1}^{n} a_k + b$ où $\prod_{k=1}^{n} a_k \in \bigcap_{k=1}^{n} I_k$ et $b \in J$. Donc $\bigcap_{k=1}^{n} I_k$ et J sont comaximaux. ■

Théorème 2.44 (Théorème des restes chinois)**.**
Soient $(A, 0, 1, +, \cdot)$ un anneau commutatif et $I_1, \dots, I_n \subset A$ des idéaux de A deux à deux comaximaux.

Alors $f : \begin{array}{ccc} A & \to & A/I_1 \times \cdots \times A/I_n \\ x & \mapsto & \left(x \mod I_1, \dots, x \mod I_n\right) \end{array}$ *est un morphisme d'anneaux surjectif de noyau $\bigcap_{k=1}^{n} I_k$.*

Démonstration. Il est clair que $f : \begin{array}{ccc} A & \to & A/I_1 \times \cdots \times A/I_n \\ x & \mapsto & \left(x \mod I_1, \dots, x \mod I_n\right) \end{array}$ est un morphisme d'anneaux et que $\ker(f) = \bigcap_{k=1}^{n} I_k$.
Montrons la surjectivité par récurrence sur $n \in \mathbb{N} \setminus \{0\}$.

- Si $n = 1$ alors $f : A \to A/I_1$ est la projection canonique qui est surjective.
- Si $n = 2$ alors, puisque I_1 et I_2 sont comaximaux, il existe $a_1 \in I_1$ et $a_2 \in I_2$ tels que $1 = a_1 + a_2$.
  Soient $y_1 \in A/I_1$ et $y_2 \in A/I_2$.
  Alors il existe $x_1, x_2 \in A$ tels que $y_1 = \overline{x_1}$ et $y_2 = \overline{x_2}$. Posons $x := x_1 a_2 + x_2 a_1$.
  Alors, on a $x = x_1(1 - a_1) + x_2 a_1 \equiv x_1 \mod I_1$ et $x = x_1 a_2 + x_2(1 - a_2) \equiv x_2 \mod I_2$.
  Donc $f(x) = (y_1, y_2)$.
- Supposons l'énoncé vrai pour un certain $n \geq 2$.
  Soient $I_1, \dots, I_n, I_{n+1} \subset A$ des idéaux de A deux à deux comaximaux.
  Soient $(y_1, \dots, y_n, y_{n+1}) \in A/I_1 \times \cdots \times A/I_n \times A/I_{n+1}$.
  Par hypothèse de récurrence, il existe $x \in A$ tel que, pour $k \in \{1, \dots, n\}$, $\overline{x} = y_k \in A/I_k$.
  D'après le lemme, $\bigcap_{k=1}^{n} I_k$ et I_{n+1} sont comaximaux. Donc, d'après le cas $n = 2$, il existe $x' \in A$ tel que $\overline{x'} = \overline{x}$ dans $A\big/\bigcap_{k=1}^{n} I_k$ et $\overline{x'} = y_{n+1}$ dans A/I_{n+1}. Ainsi

$$\begin{aligned} f(x') &= \left(x' \mod I_1, \dots, x' \mod I_n, x' \mod I_{n+1}\right) \\ &= \left(x \mod I_1, \dots, x \mod I_n, y_{n+1}\right) \\ &= (y_1, \dots, y_n, y_{n+1}). \end{aligned}$$

■

Corollaire 2.45. *Soient $(A, 0, 1, +, \cdot)$ un anneau commutatif et $I_1, \dots, I_n \subset A$ des idéaux de A deux à deux comaximaux. Alors $A\big/\bigcap_{k=1}^{n} I_k$ et $A/I_1 \times \cdots \times A/I_n$ sont isomorphes.*

Définition 2.46. Soient $(A, 0, 1, +, \cdot)$ un anneau commutatif et $a, b \in A$. On dit que a et b sont *étrangers* s'il existe $u, v \in A$ tels que $1 = au + bv$.

Exemple 2.47. D'après le théorème de Bézout, $m, n \in \mathbb{Z}$ sont étrangers si et seulement si $\text{pgcd}(m, n) = 1$.

Lemme 2.48. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a,b\in A$.*
Alors a et b sont étrangers si et seulement si (a) et (b) sont comaximaux.

Démonstration. a et b sont étrangers si et seulement si $1\in(a)+(b)$ si et seulement si $(a)+(b)=A$. ■

Lemme 2.49. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a_1,\dots,a_n\in A$ des éléments de A deux à deux étrangers alors $\bigcap_{k=1}^{n}(a_k)=(a_1\cdots a_n)$.*

Démonstration. Montrons le résultat par récurrence sur $n\in\mathbb{N}\setminus\{0\}$.

- Si $n=1$, il n'y a rien à démontrer.
- Si $n=2$: soient $a_1,a_2\in A$ étrangers.
  - ⋆ $a_1a_2\in(a_1)$ et $a_1a_2\in(a_2)$ ainsi $a_1a_2\in(a_1)\cap(a_2)$.
    De plus $(a_1)\cap(a_2)$ est un idéal comme intersection de deux idéaux, donc $(a_1a_2)\subset(a_1)\cap(a_2)$.
  - ⋆ Soit $x\in(a_1)\cap(a_2)$. Alors il existe $b_1,b_2\in A$ tels que $x=a_1b_1=a_2b_2$.
    Puisque a_1 et a_2 sont étrangers, il existe $u_1,u_2\in A$ tels que $1=a_1u_1+b_2u_2$.
    Alors $x=a_1u_1x+a_2u_2x=a_1a_2(u_1b_2+u_2b_1)\in(a_1a_2)$.
- Supposons le résultat vrai pour un certain $n\geq 2$.
  Soient $a_1,\dots,a_n,a_{n+1}\in A$ des éléments de A deux à deux étrangers.
  Par hypothèse de récurrence, $\bigcap_{k=1}^{n}(a_k)=(a_1\cdots a_n)$.
  D'après les Lemmes 2.43 et 2.48, $(a_1\cdots a_n)=\bigcap_{k=1}^{n}(a_k)$ et (a_{n+1}) sont comaximaux.
  Donc $a_1\cdots a_n$ et a_{n+1} sont étrangers, toujours d'après le Lemme 2.48.
  On déduit donc du cas $n=2$ que $\bigcap_{k=1}^{n+1}(a_k)=(a_1\cdots a_n)\cdot(a_{n+1})=(a_1\cdots a_na_{n+1})$. ■

Le résultat suivant se déduit du théorème des restes chinois à l'aide des deux lemmes précédents.

Théorème 2.50 (Théorème des restes chinois, variante)**.**
Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a_1,\dots,a_n\subset A$ des éléments de A deux à deux étrangers.
Alors $f:\begin{array}{ccc}A&\to&A/(a_1)\times\cdots\times A/(a_n)\\ x&\mapsto&\big(x \mod (a_1),\dots,x \mod (a_n)\big)\end{array}$ *est un morphisme d'anneaux surjectif de noyau $(a_1a_2\cdots a_n)$.*

Corollaire 2.51. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a_1,\dots,a_n\subset A$ des éléments de A deux à deux étrangers. Alors $A/(a_1a_2\cdots a_n)$ et $A/(a_1)\times\cdots\times A/(a_n)$ sont isomorphes.*

La démonstration de la surjectivité dans le théorème des restes chinois fournit un algorithme pour déterminer l'inverse.

Exemple 2.52. On souhaite résoudre $\begin{cases}x\equiv 2 \mod 6\\ x\equiv -1 \mod 5\\ x\equiv 3 \mod 7\end{cases}$.
Puisque 6, 5 et 7 sont deux à deux premiers entre eux, on déduit du théorème des restes chinois que le système admet une solution.
On considère la relation de Bézout $6\cdot 1+5\cdot(-1)=1$.
Alors $r:=6\cdot 1\cdot(-1)+5\cdot(-1)\cdot 2=-16$ vérifie $r\equiv 2 \mod 6$ et $r\equiv -1 \mod 5$.
On considère la relation de Bézout $30\cdot(-3)+7\cdot 13=1$ (où $30=6\cdot 5$).
Alors $x:=30\cdot(-3)\cdot 3+7\cdot 13\cdot(-16)=-1726$ vérifie $r\equiv 2 \mod 6$, $r\equiv -1 \mod 5$ et $r\equiv 3 \mod 7$.
D'après le théorème des restes chinois, l'ensemble des solutions est donc $\{-1726+6\cdot 5\cdot 7\cdot r\ :\ r\in\mathbb{Z}\}=\{-1726+210r\ :\ r\in\mathbb{Z}\}=\{-46+210s\ :\ s\in\mathbb{Z}\}$.

Exemple 2.53. D'après le théorème des restes chinois, $\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ induit un isomorphisme $f : \mathbb{Z}/84\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. On souhaite expliciter f^{-1}.
En résolvant le système $\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 0 \mod 4 \\ x \equiv 0 \mod 7 \end{cases}$, on trouve que $f^{-1}\left(\overline{1},\overline{0},\overline{0}\right) = \overline{28}$.
De même, on obtient que $f^{-1}\left(\overline{0},\overline{1},\overline{0}\right) = \overline{21}$ et que $f^{-1}\left(\overline{0},\overline{0},\overline{1}\right) = \overline{36}$.
Donc $f^{-1}\left(\overline{x},\overline{y},\overline{z}\right) = \overline{28x+21y+36z}$.

2.7 Anneaux noethériens

Définition 2.54. Un anneau *noethérien* est un anneau commutatif dont tout idéal est finiment engendré.

Exemples 2.55.

- Tout anneau principal est noethérien, par exemple $\mathbb{Z}$ et $\mathbb{R}[X]$.
- $\mathbb{Z}\left[\sqrt{d}\right]$ est noethérien, où $d \in \mathbb{Z}$.
  En effet, soit I un idéal de $\mathbb{Z}\left[\sqrt{d}\right]$. Pour tout $a \in I$, il existe $m_a, n_a \in \mathbb{Z}$ tels que $a = m_a + n_a\sqrt{d}$.
  Puisque $\mathbb{Z}$ est principal, il existe $m \in \mathbb{Z}$ tel que $\left(\{m_a \ : \ a \in I\}\right) = (m)$.
  Donc, pour tout $a \in A$, il existe $\tilde{m}_a \in \mathbb{Z}$ tel que $a = m\tilde{m}_a + n_a\sqrt{d}$.
  Puisque $m \in (m) = \left(\{m_a \ : \ a \in I\}\right)$, il existe $r \in \mathbb{N}$, $u_1, \dots, u_r \in \mathbb{Z}$ et $a_1, \dots, a_r \in I$ tels que $m = u_1 m_{a_1} + \cdots + u_r m_{a_r}$.
  Posons $y \coloneqq u_1 a_1 + \cdots + u_r a_r \in I$ alors $y = m + n\sqrt{d}$ où $n = u_1 n_{a_1} + \cdots + u_r n_{a_r} \in \mathbb{Z}$.
  Ainsi, pour tout $a \in I$, $a - \tilde{m}_a y = \tilde{n}_a\sqrt{d}$ où $\tilde{n}_a = n_a + \tilde{m}_a n \in \mathbb{Z}$.
  Puisque $\mathbb{Z}$ est principal, il existe $\tilde{n} \in \mathbb{Z}$ tel que $\left(\{\tilde{n}_a \ : \ a \in I\}\right) = (\tilde{n})$.
  Il existe alors $s \in \mathbb{N}$, $v_1, \dots, v_s \in A$ et $b_1, \dots, b_s \in I$ tels que $\tilde{n} = v_1 n_{b_1} + \cdots + v_s n_{b_s}$.
  Donc $z \coloneqq \tilde{n}\sqrt{d} \in I$.
  Soit $a \in I$ alors $\tilde{n}_a \in (\tilde{n})$, donc il existe $\tilde{\tilde{n}}_a \in \mathbb{Z}$ tel que $\tilde{n}_a = \tilde{n}\tilde{\tilde{n}}_a$. Ainsi $a = \tilde{m}_a y + \tilde{\tilde{n}}_a z$.
  Donc $I = (y, z)$ et $\mathbb{Z}\left[\sqrt{d}\right]$ est noethérien.

  On verra dans la suite une démonstration plus simple utilisant le théorème de la base de Hilbert.

Proposition 2.56. *Soit $(A, 0, 1, +, \cdot)$ un anneau commutatif, alors les énoncés suivants sont équivalents :*
(1) *A est noethérien.*
(2) *Toute suite croissante (pour l'inclusion) d'idéaux de A est stationnaire,*
i.e. si $(I_n)_{n\in\mathbb{N}}$ est une suite d'idéaux de A vérifiant $\forall n \in \mathbb{N}$, $I_n \subset I_{n+1}$ alors il existe $N \in \mathbb{N}$ tel que $\forall n \in \mathbb{N}$, $n \geq N \implies I_n = I_N$.
(3) *Toute ensemble non vide d'idéaux de A admet un élément maximal (pour l'inclusion),*
i.e. si $\mathscr{F} \neq \emptyset$ est un ensemble non vide d'idéaux de A alors $\exists I \in \mathscr{F}$, $\forall J \in \mathscr{F}$, $I \subset J \implies I = J$.

Démonstration.

(1)⇒(2) Supposons que A soit noethérien.
Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A. Posons $I \coloneqq \bigcup_{n\in\mathbb{N}} I_n$, alors I est un idéal de A.
En effet, $I \neq \emptyset$ puisque $0 \in I_0 \subset I$.
Soient $x_1, x_2 \in I$ et $a \in A$. Alors il existe $n_1, n_2 \in \mathbb{N}$ tels que $x_1 \in I_{n_1}$ et $x_2 \in I_{n_2}$.
Posons $n \coloneqq \max(n_1, n_2)$, alors $x_1, x_2 \in I_n$. Donc $x_1 + ax_2 \in I_n$ puisque I_n est un idéal.
Enfin $x_1 + ax_2 \in I_n \subset \bigcup_{n\in\mathbb{N}} I_n = I$.
Donc, par hypothèse, I est finiment engendré, i.e. il existe $a_1, \dots, a_r \in I$ tels que $I = (a_1, \dots, a_r)$.
Soit $i \in \{1, \dots, r\}$ alors il existe $m_i \in \mathbb{N}$ tel que $a_i \in I_{m_i}$.
Posons $N \coloneqq \max(m_1, \dots, m_r)$, alors $\forall i \in \{1, \dots, r\}$, $a_i \in I_{m_i} \subset I_N$ et donc $I = (a_1, \dots, a_r) \subset I_N$.
Soit $n \geq N$ alors $I \subset I_N \subset I_n \subset I$. Donc $I_n = I_N$.

(2)⇒(3) On va montrer la contraposée. Supposons qu'il existe $\mathscr{F}$ un ensemble non vide d'idéaux de A n'admettant pas d'élément maximal.
Puisque $\mathscr{F}$ est non vide, il existe $I_0 \in \mathscr{F}$.
Supposons qu'il existe $I_1, \dots, I_n \in \mathscr{F}$ tels que $I_1 \subsetneq \cdots \subsetneq I_n$.
Puisque $\mathscr{F}$ n'admet pas d'élément maximal, il existe $I_{n+1} \in \mathscr{F}$ tel que $I_{n+1} \supsetneq I_n$.
On a donc construit par récurrence une suite $(I_n)_{n\in\mathbb{N}}$ strictement croissante d'idéaux de A.

(3)⇒(1) Supposons que tout ensemble non vide d'idéaux de A admet un élément maximal.
Soit I un idéal de A. Considérons

$$\mathscr{F} \coloneqq \left\{ J \ : \ J \text{ idéal finiment engendré de } A \text{ inclus dans } I \right\}.$$

Puisque $\{0\} \in \mathscr{F}$, on a $\mathscr{F} \neq \varnothing$. Donc $\mathscr{F}$ admet un élément maximal J.
Comme $J \in \mathscr{F}$, on a $J \subset I$. Supposons par l'absurde que $J \neq I$ alors il existe $a \in I \setminus J$.
Donc $J \subsetneq J + (a)$ et $J + (a) \in \mathscr{F}$. D'où une contradiction avec la maximalité de J.
Ainsi $I = J$ est finiment engendré. ■

Exemple 2.57. L'anneau $\mathcal{C}^0(\mathbb{R},\mathbb{R})$ n'est pas noethérien puisque $I_n \coloneqq \left\{ f \in \mathcal{C}^0(\mathbb{R},\mathbb{R}) \ : \ f_{|[n,+\infty[} \equiv 0 \right\}$ définit une suite $(I_n)_{n\in\mathbb{N}}$ strictement croissante d'idéaux de $\mathcal{C}^0(\mathbb{R},\mathbb{R})$.

Proposition 2.58. *Soit $f : A \to B$ un morphisme d'anneaux surjectif. Si A est noethérien alors B l'est aussi.*

Démonstration.

- Montrons que B est commutatif.
  Soient $b_1, b_2 \in B$. Puisque f est surjectif, il existe $a_1, a_2 \in A$ tels que $b_1 = f(a_1)$ et $b_2 = f(a_2)$.
  Ainsi $b_1 b_2 = f(a_1)f(a_2) = f(a_1 a_2) = f(a_2 a_1) = f(a_2)f(a_1) = b_2 b1$ puisque A est commutatif.

- Montrons que tout idéal de B est finiment engendré.
  Soit I un idéal de B. Alors $f^{-1}(I)$ est un idéal de A et il existe donc $a_1, \dots, a_n \in A$ tels que $f^{-1}(I) = (a_1, \dots, a_n)$ puisque A est noethérien.
  Puisque f est surjectif, on a $I = f\left(f^{-1}(I)\right) = f\left((a_1, \dots, a_n)\right)$. Montrons que $I = \left(f(a_1), \dots, f(a_n)\right)$.
  Pour $i \in \{1, \dots, n\}$, on a $f(a_i) \in f\left((a_1, \dots, a_n)\right) = I$. Donc $\left(f(a_1), \dots, f(a_n)\right) \subset I$.
  Soit $x \in I = f\left((a_1, \dots, a_n)\right)$ alors il existe $u_1, \dots, u_n \in A$ tels que $x = f(u_1 a_1 + \cdots + u_n a_n) = f(u_1)f(a_1) + \cdots + f(u_n)f(a_n) \in \left(f(a_1), \dots, f(a_n)\right)$. Donc $I = \left(f(a_1), \dots, f(a_n)\right)$ ■

Corollaire 2.59. *Si A est un anneau noethérien et si I est un idéal de A alors A/I est un anneau noethérien.*

Démonstration. Soient A un anneau noethérien et I un idéal de A. Comme la projection canonique $\pi : A \to A/I$ est un morphisme d'anneaux surjectif, on déduit de la proposition précédente que A/I est un anneau noethérien. ■

Exemple 2.60. $\mathbb{Z}/10\mathbb{Z}$ est un anneau noethérien non-intègre.

Corollaire 2.61. *Soient A et B deux anneaux isomorphes. Alors A est noethérien si et seulement B l'est.*

Théorème 2.62 (Théorème de la base de Hilbert)**.** *Si A est un anneau noethérien alors $A[X]$ l'est aussi.*

Démonstration. Soit A un anneau noethérien et I un idéal de $A[X]$.
Supposons par l'absurde que I ne soit pas finiment engendré.
Il existe $f_0 \in I \setminus \{0\}$ de degré minimal. Supposons $f_1, \dots, f_n$ déjà construits alors, par hypothèse, il existe $f_{n+1} \in I \setminus (f_0, \dots, f_n)$ de degré minimal.
On a donc construit $(f_n)_{n\in\mathbb{N}}$ une suite d'éléments de I telle que $\forall n \in \mathbb{N}$, $f_{n+1} \in I \setminus (f_0, \dots, f_n)$ et $\left(\deg(f_n)\right)_{n\in\mathbb{N}}$ est une suite croissante d'entiers naturels.
Pour tout $n \in \mathbb{N}$, notons a_n le coefficient dominant de f_n, alors $(a_0) \subset (a_0, a_1) \subset (a_0, a_1, a_2) \subset \cdots$ est une suite croissante d'idéaux de A. Elle est donc stationnaire : il existe $N \in \mathbb{N} \setminus \{0\}$ tel que

$$\forall n \in \mathbb{N},\ n \geq N \implies (a_0, \dots, a_n) = (a_0, \dots, a_{N-1}).$$

Puisque $a_N \in (a_0, \dots, a_{N-1})$, il existe $u_0, \dots, u_{N-1} \in A$ tels que $a_N = u_0 a_0 + \cdots + u_{N-1} a_{N-1}$.
Posons $g \coloneqq \sum_{i=0}^{N-1} u_i X^{\deg(f_N)-\deg f_i} f_i \in A[X]$.
Alors $\deg(g) = \deg(f_N)$, le coefficient dominant de g est a_N et $g \in (f_1, \dots, f_{N-1})$.
De plus $f_N - g \in I \setminus (f_0, \dots, f_{N-1})$ puisque sinon $f_N = (f_N - g) + g \in (f_1, \dots, f_{N-1})$.
Mais $\deg(f_N - g) < \deg(f_N)$, d'où une contradiction avec la minimalité du degré de f_N. ■

Corollaire 2.63. *Si A est un anneau noethérien alors $A[X_1, \dots, X_n]$ l'est aussi.*

Démonstration. On démontre le résultat par récurrence on remarquant que

$$A[X_1, \dots, X_n, X_{n+1}] \simeq A[X_1, \dots, X_n][X_{n+1}].$$

■

Exemple 2.64. $\mathbb{Z}\left[\sqrt{d}\right]$ est noethérien, où $d \in \mathbb{Z}$.

En effet, $\mathbb{Z}[X]$ est noethérien d'après le théorème de la base de Hilbert et $\begin{array}{ccc} \mathbb{Z}[X] & \to & \mathbb{Z}\left[\sqrt{d}\right] \\ P & \mapsto & P\left(\sqrt{d}\right) \end{array}$ est un morphisme d'anneaux surjectif.

Exercices

Exercice 2.1.
On considère $C^0([0,1])$ l'anneau des fonctions $f : [0,1] \to \mathbb{R}$ continues.
Montrer de deux façons différentes que $I := \{f \in C^0([0,1]) \ : \ f(0) = 0\}$ 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 2.2. Montrer que les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Exercice 2.3.
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 2.4.
(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 2.5.
On définit l'ensemble des nombres décimaux par $\mathbb{D} := \left\{ \frac{a}{10^k} \ : \ a \in \mathbb{Z},\ k \in \mathbb{N} \right\}$.
(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 2.6.
On considère $I := (2, X)$ 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 2.7. Soient A un anneau commutatif et I un idéal de A.
On définit le *radical* de I par $\sqrt{I} := \{x \in A \ : \ \exists n \in \mathbb{N} \setminus \{0\},\ x^n \in I\}$.
(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 2.8. 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 2.9. *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 2.10 (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 $\operatorname{car}(A)$, 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 $\operatorname{car}(A)=0$ (on dit alors que A est de *caractéristique nulle*).

(3) Déterminer la caractéristique des anneaux suivants :
   (a) $\mathbb{Z}$
   (b) $\mathbb{Z}/n\mathbb{Z}$ où $n\in\mathbb{N}$
   (c) $\mathbb{Q}$
   (d) $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$
   (e) $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$
   (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 $p:=\operatorname{car}(A)$ est un nombre premier.
   (a) Montrer que $\forall k\in\{1,\dots,p-1\},\ p\big|\binom{p}{k}$.
   (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 2.11.

(1) Déterminer les idéaux premiers de $\mathbb{Z}$.
(2) Déterminer les idéaux maximaux de $\mathbb{Z}$.

Exercice 2.12. 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 2.13. 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 2.14.
On considère l'unique morphisme d'anneaux $\Theta : \mathbb{Z}\to\mathbb{Z}[i]/(i-3)$, i.e. $\Theta(n):=\overline{n}$.

(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 2.15.
Soit A un anneau de Boole (voir l'Exercice 1.16).
(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 2.16.
(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 2.17.
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 2.18. 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 2.19.
Montrer que si A est un anneau commutatif alors $A \setminus A^*$ est la réunion des idéaux maximaux de A.

Exercice 2.20.
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 2.21.
(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 2.22.
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 2.23.
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) $\mathbb{R}[X]/(X^4 + X^2) \to \mathbb{R}[X]/(X^2) \times \mathbb{R}[X]/(X^2 + 1)$

Exercice 2.24. L'objectif de cet exercice est d'étudier l'anneau $A \coloneqq \mathbb{Z} \times \mathbb{Z}$.
(1) Dire si les énoncés suivants sont vrais ou faux en justifiant.
  (a) A est commutatif.
  (b) A est intègre.
(2) Déterminer l'ensemble A^* des inversibles de A.

Pour $d \in \mathbb{N}$, on note $A_d \coloneqq \{(x, y) \in A \ : \ d | y - x\}$.
(3) Montrer que, pour tout $d \in \mathbb{N}$, A_d est un sous-anneau de A.
(4) L'objectif de cette question est de montrer que, réciproquemment, tout sous-anneau de A est de la forme A_d avec $d \in \mathbb{N}$.
  Soit B un sous-anneau de A.
  (a) Montrer que $H \coloneqq \{x \in \mathbb{Z} \ : \ (x, 0) \in B\}$ est un sous-groupe de $\mathbb{Z}$.
  (b) Soit $(x, y) \in A$. Montrer que $(x, y) \in B$ si et seulement si $(x - y, 0) \in B$.
  (c) Déduire des questions précédentes qu'il existe $d \in \mathbb{N}$ tel que $B = A_d$.
(5) Soient I_1 et I_2 deux idéaux de $\mathbb{Z}$.
  (a) Montrer que $I_1 \times I_2$ est un idéal de A.
  (b) Montrer que $A/(I_1 \times I_2)$ et $\left(\mathbb{Z}/I_1\right) \times \left(\mathbb{Z}/I_2\right)$ sont isomorphes.
  (c) Déterminer un idéal maximal de A.
  (d) Déterminer un idéal premier de A qui n'est pas maximal.
(6) Le but de cette question est de montrer que, réciproquemment, tout idéal de A est de la forme $I_1 \times I_2$.
  Soit I un idéal de A. On note $I_1 \coloneqq \{x \in \mathbb{Z} \ : \ (x, 0) \in I\}$ et $I_2 \coloneqq \{y \in \mathbb{Z} \ : \ (0, y) \in I\}$.
  (a) Montrer que I_1 est un idéal de $\mathbb{Z}$.
    On admettra dans la suite que I_2 est aussi un idéal de $\mathbb{Z}$.
  (b) Montrer que $I = I_1 \times I_2$.
  (c) En déduire que I est principal.
  (d) L'anneau A est-il principal ?

3 Divisibilité dans les anneaux

3.1 Divisibilité

Définition 3.1. Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a,b\in A$.
On dit que *a divise b* (ou que a est un *diviseur* de b ou que b est un *multiple* de a), noté $a|b$, s'il existe $x\in A$ tel que $b=ax$.

Remarque 3.2. Tout élément de A divise 0 : si $a\in A$ alors $0=a\cdot 0$.
La terminologie porte à confusion : il ne faut pas confondre avec la notion de *diviseur de zéro* de la Définition 1.25...
Pour lever l'ambigüité, on écrit *diviseur de zéro* (avec *zéro* en toute lettre) pour la notion de la Définition 1.25 (attention, ce n'est pas une convention standard).

Exemples 3.3.

- Soit $(A,0,1,+,\cdot)$ un anneau commutatif, alors
  - $\star$ $\forall a\in A$, $a|0$ (puisque si $a\in A$ alors $0=a\cdot 0$),
  - $\star$ $\forall a\in A\setminus\{0\}$, $0\nmid a$ (par contraposée, supposons que $0|a$ alors il existe $x\in A$ tel que $a=0x$, donc $a=0$),
  - $\star$ $\forall u\in A^*$, $\forall a\in A$, $u|a$ (puisque si $a\in A$ et $u\in A^*$ alors $a=uu^{-1}a$).
- Dans $\mathbb{Z}$:
  - $\star$ $2|6$,
  - $\star$ $2\nmid 3$ (sinon il existerait $x\in\mathbb{Z}$ tel que $3=2x$ d'où $1\equiv 0 \mod 2$, contradiction).
- Dans $\mathbb{Q}$: $2|3$ (puisque $3=2\cdot\frac{3}{2}$).
- Dans $\mathbb{Z}[i]$:
  - $\star$ $2\nmid 1+i$ (sinon il existerait $a,b\in\mathbb{Z}$ tels que $1+i=2a+2ib$ d'où $1=2a\equiv 0 \mod 2$, contradiction),
  - $\star$ $1+i|2$ (puisque $(1+i)(1-i)=2$).

Proposition 3.4. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $d,a,b\in A$.*
Si $d|a$ et $d|b$ alors d divise toute combinaison linéaire de a et b, i.e. $\forall u,v\in A$, $d|au+bv$.

Démonstration. Supposons que $d|a$ et $d|b$. Alors il existe $\alpha,\beta\in A$ tels que $a=d\alpha$ et $b=d\beta$.
Soient $u,v\in A$. Alors $au+bv=d\alpha u+d\beta v=d(\alpha u+\beta v)$. Donc $d|au+bv$. ■

Proposition 3.5. *Soit $(A,0,1,+,\cdot)$ un anneau commutatif, alors $\forall a\in A$, $a\in A^*\Leftrightarrow a|1$.*

Démonstration. Soit $a\in A$.
⇒ Si $a\in A^*$ alors il existe $u\in A$ tel que $1=au$. Donc $a|1$.
⇐ Si $a|1$ alors il existe $u\in A$ tel que $1=au$. Donc $a\in A^*$. ■

Proposition 3.6. *Soit $(A,0,1,+,\cdot)$ un anneau commutatif, alors*

$$\forall a,b\in A,\ a|b\Leftrightarrow (b)\subset(a).$$

Démonstration. Soient $a,b\in A$.

⇒ Supposons que $a|b$, alors il existe $u\in A$ tel que $b=au$.
Soit $x\in(b)$ alors il existe $v\in A$ tel que $x=bv$. Donc $x=bv=auv\in(a)$.
Donc $(b)\subset(a)$.

⇐ Supposons que $(b)\subset(a)$.
Alors $b\in(b)\subset(a)$. Donc il existe $x\in A$ tel que $b=ax$. Ainsi $a|b$. ■

Définition 3.7. Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a,b\in A$.
On dit que a et b sont *premiers entre eux* si les seuls diviseurs communs à a et b sont les inversibles, i.e.

$$\forall d\in A,\ d|a \text{ et } d|b \implies d\in A^*.$$

Proposition 3.8. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a,b\in A$.*
Si a et b sont étrangers alors a et b sont premiers entre eux.

Démonstration. Supposons que a et b soient étrangers. Alors il existe $u,v\in A$ tels que $1=au+bv$.
Puisque $d|a$ et $d|b$, on a $d|au+bv=1$. Donc $d\in A^*$. ■

Remarque 3.9. La réciproque est fausse : 2 et X sont premiers entre eux dans $\mathbb{Z}[X]$ mais ils ne sont pas étrangers puisque $1\notin(2,X)$, voir l'Exercice 2.6.

3.2 Association

Définition 3.10. Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a,b\in A$. On dit que a et b sont *associés* si $a|b$ et $b|a$.

Proposition 3.11. *L'association est une relation d'équivalence.*

Démonstration. Soit $(A,0,1,+,\cdot)$ un anneau commutatif.
- *Réflexivité :* soit $a\in A$ alors $a|a$, donc a et a sont associés.
- *Symétrie :* soient $a,b\in A$ tels que a et b sont associés, alors $b|a$ et $a|b$ donc b et a sont associés.
- *Transitivité :* soient $a,b,c\in A$ tels que a et b sont associés et b et c sont associés.
  Alors $a|b$ et $b|c$ donc $a|c$. De même $b|a$ et $c|b$ donc $c|a$. Ainsi a et c sont associés. ■

Proposition 3.12. *La divisibilité est une relation d'ordre sur les éléments de A à association près.*

Démonstration. Soit $(A,0,1,+,\cdot)$ un anneau commutatif.
- *Réflexivité :* soit $a\in A$ alors $a|a$.
- *Antisymétrie :* soient $a,b\in A$ tels que $a|b$ et $b|a$. Alors a et b sont associés.
- *Transitivité :* soient $a,b,c\in A$ tels que $a|b$ et $b|c$ alors $a|c$. ■

Proposition 3.13. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a,b\in A$.*
Alors a et b sont associés *si et seulement si $(a)=(b)$.*

Démonstration. C'est une conséquence de la Proposition 3.6. ■

Proposition 3.14. *Soient $(A,0,1,+,\cdot)$ un anneau intègre et $a,b\in A$.*
Alors a et b sont associés si et seulement s'il existe $u\in A^*$ tel que $a=bu$.

Démonstration. C'est une conséquence de la proprosition précédente et de la Proposition 2.27. ■

Remarque 3.15. Soient A un anneau commutatif et $a,b\in A$. S'il existe u inversible tel que $a=bu$ alors a et b sont associés sans hypothèse d'intégrité (voir Remarque 2.28).
En revanche, la réciproque n'est généralement pas vraie si A n'est pas supposé intègre (Exercice 3.1).

3.3 PGCD & PPCM

Définition 3.16. Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a,b\in A$.
Un *plus grand commun diviseur* (*pgcd*) de a et b est un élément $d\in A$ tel que
(i) $d|a$,
(ii) $d|b$ et
(iii) $\forall c\in A,\ c|a$ et $c|b \implies c|d$.

Proposition 3.17. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a\in A$. Alors a est un pgcd de a et 0.*

Démonstration. On a $a|a$ et $a|0$. Soit $d\in A$ tel que $d|a$ et $d|0$ alors $d|a$. Donc a est un pgcd de a et 0. ■

Remarque 3.18. En particulier 0 est un pgcd de 0 et 0.

Remarque 3.19. Deux éléments d'un anneau commutatif peuvent ne pas avoir de pgcd.
On va montrer 4 et $2\left(1+i\sqrt{3}\right)$ n'ont pas de pgcd dans $\mathbb{Z}\left[i\sqrt{3}\right]$.
Soit $x \in \mathbb{Z}\left[i\sqrt{3}\right]$ un diviseur de 4 alors il existe $u \in \mathbb{Z}\left[i\sqrt{3}\right]$ tel que $4 = xu$.
Alors $|x|^2|u|^2 = 16$, donc $\left(|x|^2, |u|^2\right) \in \{(16,1),(8,2),(4,4),(2,8),(1,16)\}$.
Notons $x = a + ib$ où $a, b \in \mathbb{Z}$, alors

- $|x|^2 = 16 \Leftrightarrow a^2+3b^2 = 16 \Leftrightarrow (b=0,\ a=\pm 4)$ ou $(b=\pm 2$ et $a=\pm 2) \Leftrightarrow x \in \left\{\pm 4,\ \pm 2 \pm 2i\sqrt{3}\right\}$
- $|x|^2 = 8 \Leftrightarrow a^2+3b^2 = 8$ n'a pas de solution.
- $|x|^2 = 4 \Leftrightarrow a^2+3b^2 = 4 \Leftrightarrow (b=0$ et $a \pm 2)$ ou $(b=\pm 1$ et $a=\pm 1) \Leftrightarrow x \in \left\{\pm 2, \pm 1 \pm i\sqrt{3}\right\}$
- $|x|^2 = 2 \Leftrightarrow a^2+3b^2 = 2$ n'a pas de solution.
- $|x|^2 = 1 \Leftrightarrow a = \pm 1 \Leftrightarrow x = \pm 1$

On vérifie que, parmi les candidats ci-dessus, les diviseurs de 4 sont ± 1, ± 2, $\pm 1 \pm i\sqrt{3}, \pm 4$.
De façon similaire, on trouve que les diviseurs de $2\left(1+i\sqrt{3}\right)$ sont $\pm 1, \pm 2, \pm\left(1+i\sqrt{3}\right), \pm 2\left(1+i\sqrt{3}\right)$.
Donc les diviseurs communs de 4 et $2\left(1+i\sqrt{3}\right)$ sont ± 1, ± 2 et $\pm\left(1+i\sqrt{3}\right)$.
On remarque que $2 \nmid 1+i\sqrt{3}$ et $1+i\sqrt{3} \nmid 2$, donc 4 et $2\left(1+i\sqrt{3}\right)$ n'ont pas de pgcd.

Remarque 3.20. S'il existe, le pgcd de deux éléments n'est généralement pas unique :

- Les pgcd de 6 et 10 dans $\mathbb{Z}$ sont -2 et 2.
- Les pgcd de $\overline{3}$ et $\overline{6}$ dans $\mathbb{Z}/8\mathbb{Z}$ sont $\overline{1}$, $\overline{3}$, $\overline{5}$ et $\overline{7}$.

En revanche, s'il existe, le pgcd de deux éléments est unique à association près, comme le montre la proposition suivante.

Proposition 3.21. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a, b, d, d' \in A$.*

- *Si d et d' sont deux pgcd de a et b alors d et d' sont associés.*
- *Si d est un pgcd de a et b et si d et d' sont associés alors d' est un pgcd de a et b.*

Démonstration.

- Supposons que d et d' soient deux pgcd de a et b.
  Alors, puisque d' est un pgcd de a et b, $d|a$ et $d|b$, on a $d|d'$.
  De même, puisque d est un pgcd de a et b, $d'|a$ et $d'|b$, on a $d'|d$.
  Donc d et d' sont associés.

- Supposons que d soit un pgcd de a et b et que d et d' soient associés.
  On a $d|a$ et $d'|d$ donc $d'|a$. De même $d'|b$.
  Soit $c \in A$ tel que $c|a$ et $c|b$. Alors $c|d$, car d est un pgcd de a et b, et $d|d'$ par association.
  Donc $c|d'$.
  On a bien montré que d' est un pgcd de a et b. ■

Proposition 3.22. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a, b \in A$.*
Alors a et b sont premiers entre eux si et seulement si 1 est un pgcd de a et b.

Démonstration.

- Supposons que a et b soient premiers entre eux.
  Soit $d \in A$ tel que $d|a$ et $d|b$. Alors $d \in A^*$. Donc il existe $u \in A$ tel que $1 = du$. Ainsi $d|1$.
  Donc 1 est un pgcd de a et b.

- Supposons que 1 soit un pgcd de a et b.
  Soit $d \in A$ tel que $d|a$ et $d|b$. Alors $d|1$. Donc il existe $u \in A$ tel que $du = 1$, i.e. $d \in A^*$. ■

Définition 3.23. Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a,b\in A$.
Un *plus petit commun multiple* (*ppcm*) de a et b est un élément $m\in A$ tel que
(i) $a|m$,
(ii) $b|m$ et
(iii) $\forall c\in A$, $a|c$ et $b|c \implies m|c$.

Proposition 3.24. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a\in A$. Alors 0 est un ppcm de a et 0.*

Démonstration. On a $a|0$ et $0|0$. Soit $c\in A$ tel que $a|c$ et $0|c$ alors $0|c$. Donc 0 est un ppcm de a et 0. ■

Remarque 3.25. En particulier 0 est un ppcm de 0 et 0.

Remarque 3.26. Deux éléments d'un anneau commutatif peuvent ne pas avoir de ppcm.
On va montrer 2 et $1+i\sqrt{3}$ n'ont pas de ppcm dans $\mathbb{Z}\left[i\sqrt{3}\right]$.
Supposons par l'absurde que 2 et $1+i\sqrt{3}$ admettent un ppcm m dans $\mathbb{Z}\left[i\sqrt{3}\right]$.
Puisque $2\cdot 2=4$ et $\left(1+i\sqrt{3}\right)\left(1-i\sqrt{3}\right)=4$, on a $2|4$ et $1+i\sqrt{3}|4$ et donc $m|4$.
Comme $2|2\left(1+i\sqrt{3}\right)$ et $1+i\sqrt{3}|2\left(1+i\sqrt{3}\right)$, on a $m|2\left(1+i\sqrt{3}\right)$.
Donc, d'après la Remarque 3.19, $m\in\left\{\pm 1,\pm 2,\pm\left(1+i\sqrt{3}\right)\right\}$ mais aucun n'est multiple commun de 2 et $1+i\sqrt{3}$. D'où une contradiction.

Remarque 3.27. S'il existe, le ppcm de deux éléments n'est généralement pas unique : les ppcm de 6 et 10 dans $\mathbb{Z}$ sont -30 et 30.
En revanche, s'il existe, le ppcm de deux éléments est unique à association près, comme le montre la proposition suivante.

La proposition suivante se démontre de façon similaire à la Proposition 3.21.

Proposition 3.28. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a,b,m,m'\in A$.*
- *Si m et m' sont deux ppcm de a et b alors m et m' sont associés.*
- *Si m est un ppcm de a et b et si m et m' sont associés alors m' est un ppcm de a et b.*

3.4 Éléments irréductibles

Définition 3.29. Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $\pi\in A$. On dit que π est *irréductible* si
(i) $\pi\notin A^*$,
(ii) $\pi\neq 0$ et
(iii) $\forall a,b\in A$, $\pi=ab \implies a\in A^*$ ou $b\in A^*$.

Exemples 3.30.

- Les irréductibles de $\mathbb{Z}$ sont les $\pm p$ où p est un nombre premier.
- Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.

Proposition 3.31. *Soient $(A,0,1,+,\cdot)$ un anneau intègre et $\pi\in A$.*
Si (π) est un idéal premier non nul alors π est irréductible.

Démonstration. Supposons que (π) soit un idéal premier non nul.
Puisque (π) est premier, on a $(\pi)\neq A$ et donc $\pi\notin A^*$ d'après la Proposition 2.27.
Puisque $(\pi)\neq\{0\}$, on a $\pi\neq 0$.
Soient $a,b\in A$ tels que $\pi=ab$. Alors $ab\in(\pi)$ et donc $a\in(\pi)$ ou $b\in(\pi)$ puisque (π) est premier.
Supposons sans perte de généralité que $a\in(\pi)$ alors il existe $x\in A$ tel que $a=\pi x$.
D'où $0=\pi-ab=\pi-\pi xb=\pi(1-xb)$. Puisque A est intègre et $\pi\neq 0$, on a $1-xb=0$ et donc $xb=1$.
Donc $b\in A^*$. ■

Remarque 3.32. Le résultat précédent n'est pas vrai si A n'est pas supposé intègre, voir l'Exercice 3.5.
La réciproque est généralement fausse, voir l'Exercice 3.7.
En revanche, la réciproque est vraie pour les anneaux factoriels, que l'on présente dans la section suivante.

3.5 Anneaux factoriels

Définition 3.33. On dit qu'un anneau $(A,0,1,+,\cdot)$ est *factoriel* si
(0) A est intègre,
(E) Tout élément $a \in A\setminus\{0\}$ non nul peut s'écrire $a = u\pi_1\pi_2\dots\pi_r$ où $u \in A^*$ et les π_i sont irréductibles,
(U) La décomposition du point précédent est unique à permutation et association près,
i.e. si $a \in A\setminus\{0\}$ s'écrit

$$a = u\pi_1\pi_2\dots\pi_r = v\tilde{\pi}_1\tilde{\pi}_2\cdots\tilde{\pi}_s$$

où $u,v \in A^*$ et les π_i et $\tilde{\pi}_i$ sont irréductibles alors $r = s$ et il existe $\sigma \in \mathfrak{S}_r$ tel que pour tout $i \in \{1,\dots,r\}$, π_i et $\tilde{\pi}_{\sigma(i)}$ sont associés.

Exemples 3.34.

- L'anneau $\mathbb{Z}$ est factoriel (décomposition des entiers en facteurs premiers).
- L'anneau $\mathbb{Z}\left[i\sqrt{3}\right]$ n'est pas factoriel car $4 = 2\cdot 2 = \left(1+i\sqrt{3}\right)\left(1-i\sqrt{3}\right)$ alors que 2 et $1+i\sqrt{3}$ ne sont pas associés.

Proposition 3.35. *Un anneau noethérien intègre vérifie* (E).

Démonstration. Soit $(A,0,1,+,\cdot)$ un anneau noethérien intègre.
Posons $\mathcal{F} := \big\{(a) \,:\, a \in A\setminus\{0\} \text{ ne vérifie pas la décomposition (E)}\big\}$.
Supposons par l'absurde que $\mathcal{F} \neq \emptyset$.
Alors, par noethérianité, $\mathcal{F}$ admet un élément maximal (a_0) où $a_0 \in A\setminus\{0\}$ n'admet pas de décomposition en irréductibles. On remarque que
- $a_0 \neq 0$,
- $a_0 \notin A^*$ (sinon a_0 vérifierait (E)) et
- a_0 n'est pas irréductible (sinon a_0 vérifierait (E)).

Il existe donc $b,c \in A$ non nuls et non inversibles tels que $a_0 = bc$.
Si b et c vérifient (E) alors a aussi. Supposons sans perte de généralité que b ne vérifie pas (E).
Alors $(b) \in \mathcal{F}$ et $(a_0) \subset (b)$. Donc $(b) = (a_0)$ par maximalité.
Puisque A est intègre, on déduit de la Proposition 2.27 qu'il existe $u \in A^*$ tel que $a_0 = bu$.
Alors $b(c-u) = bc - bu = a_0 - a_0 = 0$ et donc $c - u = 0$ puisque $b \neq 0$ et que A est intègre.
Donc $c = u \in A^*$. D'où une contradiction. Ainsi $\mathcal{F} = \emptyset$ et A vérifie (E). ∎

Remarque 3.36. Un anneau noethérien intègre peut ne pas vérifier (U) : nous avons déjà vu que $\mathbb{Z}\left[i\sqrt{3}\right]$ est noethérien et intègre mais qu'il n'est pas factoriel.

Définition 3.37. Soit $(A,0,1,+,\cdot)$ un anneau intègre.
Un *système de représentants des irréductibles* (*sri*) *de* A est une partie $\mathcal{P} \subset A$ telle que
(i) Si $\pi \in \mathcal{P}$ alors π est irréductible,
(ii) Si $a \in A$ irréductible alors il existe $\pi \in \mathcal{P}$ tels que a et π sont associés et
(iii) Si π_1 et π_2 sont deux éléments distincts de $\mathcal{P}$ alors π_1 et π_2 ne sont pas associés.

Exemple 3.38. L'ensemble des irréductibles de $\mathbb{Z}$ est $\big\{\pm p \,:\, p \text{ premier}\big\}$ et $\mathbb{Z}^* = \{\pm 1\}$.
Ainsi $\big\{p \,:\, p \text{ premier}\big\}$, $\big\{-p \,:\, p \text{ premier}\big\}$, $\{-2,3,-5,7,\dots\}$ sont des sri de $\mathbb{Z}$.

Remarque 3.39. On admet que tout anneau intègre admet un sri (ce résultat utilise l'axiome du choix).

On obtient alors facilement la caractérisation suivante :

Proposition 3.40. *Soient $(A,0,1,+,\cdot)$ un anneau intègre et $\mathcal{P}$ un sri de A.*
Alors A est factoriel si et seulement si, pour tout $a\in A\setminus\{0\}$, il existe un unique $u\in A^*$ et une unique suite $\big(v_\pi(a)\big)_\pi\in\mathbb{N}^{\mathcal{P}}$ à support fini tels que $a=u\displaystyle\prod_{\pi\in\mathcal{P}}\pi^{v_\pi(a)}$.

Remarque 3.41. Soient $(A,0,1,+,\cdot)$ un anneau factoriel, $\mathcal{P}$ un sri de A et $\pi\in\mathcal{P}$.
On pose, par convention, $v_\pi(0)=+\infty$. La fonction $v_\pi : A\to\mathbb{N}\cup\{+\infty\}$ s'appelle la *valuation π-adique*.

Proposition 3.42. *Soient $(A,0,1,+,\cdot)$ un anneau factoriel, $\mathcal{P}$ un sri de A et $\pi\in\mathcal{P}$. Alors*
(1) $\forall a\in A,\ a=0\Leftrightarrow v_\pi(0)=+\infty$,
(2) $\forall a\in A,\ v_\pi(a)\geq 1\Leftrightarrow \pi|a$,
(3) $\forall a,b\in A,\ v_\pi(ab)=v_\pi(a)+v_\pi(b)$,
(4) $\forall a,b\in A,\ v_\pi(a+b)\geq\min\big(v_\pi(a),v_\pi(b)\big)$,
(5) $\forall a,b\in A,\ v_\pi(a+b)=\min\big(v_\pi(a),v_\pi(b)\big)\Leftrightarrow v_\pi(a)\neq v_\pi(b)$.

Démonstration.

(1) Ce point est vrai par définition de v_π.

(2) Soit $a\in A$. Si $a=0$ alors $v_\pi(a)=+\infty\geq 1$ et $\pi|a$.
On peut donc supposer que $a\neq 0$.
- ⋆ Supposons que $v_\pi(a)\geq 1$. Il existe $u\in A^*$ tel que $a=u\displaystyle\prod_{p\in\mathcal{P}}p^{v_p(a)}$. Donc $\pi|a$.
- ⋆ Supposons que $\pi|a$. Alors il existe $d\in A$ tel que $a=d\pi$.
Il existe $u\in A^*$ tel que $d=u\displaystyle\prod_{p\in\mathcal{P}}p^{v_p(d)}$. Donc $a=d\pi=u\pi\displaystyle\prod_{p\in\mathcal{P}}p^{v_p(d)}$.
Par unicité de l'écriture dans un sri, on a $v_\pi(a)=1+v_\pi(d)\geq 1$.

(3)&(4)&(5) Soient $a,b\in A$. Si $a=0$ ou $b=0$ alors les énoncés sont clairs.
On peut donc supposer que $a\neq 0$ et $b\neq 0$.
Il existe $u,v\in A^*$ tels que $a=u\displaystyle\prod_{p\in\mathcal{P}}p^{v_p(a)}$ et $b=u\displaystyle\prod_{p\in\mathcal{P}}p^{v_p(b)}$.
Alors $ab=uv\displaystyle\prod_{p\in\mathcal{P}}p^{v_p(a)+v_p(b)}$. Donc, par unicité de l'écriture dans un sri, on a $v_\pi(ab)=v_\pi(a)+v_\pi(b)$.
Et $a+b=\pi^{\min(v_\pi(a)+v_\pi(b))}\left(u\pi^{v_\pi(a)-\min(v_\pi(a)+v_\pi(b))}\displaystyle\prod_{p\in\mathcal{P}\setminus\{\pi\}}p^{v_p(a)}+v\pi^{v_\pi(b)-\min(v_\pi(a)+v_\pi(b))}\prod_{p\in\mathcal{P}\setminus\{\pi\}}p^{v_p(b)}\right)$.
Donc, par unicité de l'écriture dans un sri, on a $v_\pi(a+b)\geq\min(v_\pi(a)+v_\pi(b))$.
On a $a+b=\pi^{\min(v_\pi(a)+v_\pi(b))}\left(\pi^{v_\pi(a)-\min(v_\pi(a)+v_\pi(b))}\alpha+\pi^{v_\pi(b)-\min(v_\pi(a)+v_\pi(b))}\beta\right)$ où $\pi\nmid\alpha,\beta$.
On en déduit que $v_\pi(a+b)>\min\big(v_\pi(a),v_\pi(b)\big)\Leftrightarrow\pi\big|\pi^{v_\pi(a)-\min(v_\pi(a)+v_\pi(b))}\alpha+\pi^{v_\pi(b)-\min(v_\pi(a)+v_\pi(b))}\beta\Leftrightarrow$
$v_\pi(a)-\min(v_\pi(a)+v_\pi(b))=v_\pi(b)-\min(v_\pi(a)+v_\pi(b))\Leftrightarrow v_\pi(a)=v_\pi(b)$. ■

Proposition 3.43. *Soient $(A,0,1,+,\cdot)$ un anneau factoriel et $\mathcal{P}$ un sri de A.*
Alors $\forall a,b\in A,\ a|b\Leftrightarrow\forall\pi\in\mathcal{P},\ v_\pi(a)\leq v_\pi(b)$.

Démonstration. Soient $a,b\in A$.

- Supposons que $a|b$. Alors, il existe $x\in A$ tel que $b=ax$.
Soit $\pi\in\mathcal{P}$, alors $v_\pi(b)=v_\pi(ax)=v_\pi(a)+v_\pi(x)\geq v_\pi(a)$.

- Supposons que $\forall\pi\in\mathcal{P},\ v_\pi(a)\leq v_\pi(b)$.
Alors il existe $u,v\in A^*$ tels que $a=u\displaystyle\prod_{\pi\in\mathcal{P}}\pi^{v_\pi(a)}$ et $b=v\prod_{\pi\in\mathcal{P}}\pi^{v_\pi(b)}$.
Donc $b=v\displaystyle\prod_{\pi\in\mathcal{P}}\pi^{v_\pi(a)}\prod_{\pi\in\mathcal{P}}\pi^{v_\pi(b)-v_\pi(a)}=au^{-1}v\prod_{\pi\in\mathcal{P}}\pi^{v_\pi(b)-v_\pi(a)}$. Donc $a|b$. ■

Proposition 3.44. *Soient $(A,0,1,+,\cdot)$ un anneau factoriel et $a,b\in A$.*
Alors a et b admettent un pgcd et un ppcm.

Démonstration. Si $a=0$ ou $b=0$ alors on a déjà vu que a et b admettent un pgcd. On peut donc supposer que $a\neq 0$ et $b\neq 0$.
Soient $\mathcal{P}$ un sri de A et $d:=\prod_{\pi\in\mathcal{P}}\pi^{\min\left(v_\pi(a),v_\pi(b)\right)}$.
On a, pour tout $\pi\in\mathcal{P}$, $v_\pi(d)\leq v_\pi(a)$ et $v_\pi(d)\leq v_\pi(b)$. Donc $d|a$ et $d|b$.
Soit $c\in A$ tel que $c|a$ et $c|b$. Alors, pour tout $p\in\mathcal{P}$, $v_\pi(c)\leq v_\pi(a)$ et $v_\pi(c)\leq v_\pi(b)$.
Donc, pour tout $p\in\mathcal{P}$, on a $v_\pi(c)\leq\min\left(v_\pi(a),v_\pi(b)\right)=v_\pi(d)$. Ainsi $c|d$.
Donc d est un pgcd de a et b.
On montre de la même façon que $\prod_{\pi\in\mathcal{P}}\pi^{\max\left(v_\pi(a),v_\pi(b)\right)}$ est un ppcm de a et b. ■

Proposition 3.45. *Soit $(A,0,1,+,\cdot)$ un anneau intègre vérifiant (E) alors les énoncés suivants sont équivalents :*
(1) *A vérifie (U), i.e. A est factoriel.*
(2) Lemme d'Euclide : *soient $a,b,\pi\in A$, si π est irréductible et $\pi|ab$ alors $\pi|a$ ou $\pi|b$.*
(3) *$\forall\pi\in A$, π est irréductible $\implies(\pi)$ est premier non nul.*
(4) Lemme de Gauss : *soient $a,b,c\in A$, si $a|bc$ et si a et b sont premiers entre eux $a|c$.*

Démonstration.

(2)⇒(3) Supposons que le lemme d'Euclide soit vrai.
Soit $\pi\in A$ irréductible. Soient $a,b\in A$ tels que $ab\in(\pi)$. Alors $\pi|ab$.
D'après le Lemme d'Euclide, soit $\pi|a$ et alors $a\in(\pi)$, soit $\pi|b$ et alors $b\in(\pi)$.
De plus $(\pi)\neq\{0\}$ car $\pi\neq 0$ et $(\pi)\neq A$ car $\pi\notin A^*$ (voir Proposition 2.27).
Donc (π) est premier non nul.

(3)⇒(2) Supposons (3) et montrons le lemme d'Euclide.
Soient $a,b,\pi\in A$ tels que π est irréductible et $\pi|ab$. Alors $ab\in(\pi)$.
Donc, puisque (π) est premier, soit $a\in(\pi)$ et alors $\pi|a$, soit $b\in(\pi)$ et alors $\pi|b$.

(4)⇒(2) Supposons que le lemme de Gauss soit vrai et montrons le lemme d'Euclide.
Soient $a,b,\pi\in A$ tels que π est irréductible et $\pi|ab$.
Supposons $\pi\nmid a$. Montrons que π et a sont premiers entre eux.
Soit $d\in A$ vérifiant $d|a$ et $d|\pi$. Alors il existe $\alpha,\beta\in A$ tels que $a=d\alpha$ et $\pi=d\beta$.
Puisque π est irréductible, soit $d\in A^*$, soit $\beta\in A^*$.
Supposons par l'absurde que $\beta\in A^*$, alors $a=d\alpha=\pi\beta^{-1}\alpha$ et donc $\pi|a$, d'où une contradiction.
Par conséquent $d\in A^*$. Ainsi π et a sont premiers entre eux.
Et donc $\pi|b$ d'après le lemme de Gauss.

(2)⇒(1) Supposons le lemme d'Euclide et montrons (U).
Soient $u,v\in A^*$ et $\pi_1,\dots,\pi_r,\tilde{\pi}_1,\dots,\tilde{\pi}_s$ des irréductibles tels que $u\pi_1\pi_2\dots\pi_r=v\tilde{\pi}_1\tilde{\pi}_2\cdots\tilde{\pi}_s$.
Donc $\tilde{u}\pi_1\pi_2\dots\pi_r=\tilde{\pi}_1\tilde{\pi}_2\cdots\tilde{\pi}_s$ avec $\tilde{u}=uv^{-1}\in A^*$.
Puisque π_r est irréductible et que $\pi_r|\tilde{\pi}_1\tilde{\pi}_2\cdots\tilde{\pi}_s$, on déduit du lemme d'Euclide qu'il existe $i\in\{1,\dots,s\}$ tel que $\pi_r|\tilde{\pi}_i$. Ainsi, il existe $d\in A$ tel que $\tilde{\pi}_i=\pi_r d$.
Puisque $\tilde{\pi}_i$ est irréductible et $\pi_r\notin A^*$, on a $d\in A^*$. Donc π_r et $\tilde{\pi}_i$ sont associés.
Quitte à permuter, on peut supposer que $i=s$.
Puisque A est intègre, on a alors $\tilde{\tilde{u}}\pi_1\pi_2\dots\pi_{r-1}=\tilde{\pi}_1\tilde{\pi}_2\cdots\tilde{\pi}_{s-1}$ avec $\tilde{\tilde{u}}=\tilde{u}d^{-1}\in A^*$.
En réitérant le procédé r fois, on obtient bien (U).

(1)⇒(4) Supposons que A soit factoriel et fixons $\mathcal{P}$ un sri de A.
Soient $a,b,c\in A$ tels que $a|bc$. Montrons le résultat par contraposée.
Supposons que $a\nmid c$, alors il existe $\pi\in\mathcal{P}$ tel que $v_\pi(a)>v_\pi(c)$.
Comme $a|bc$, on a $v_\pi(a)\leq v_\pi(b)+v_\pi(c)$ et donc $v_\pi(a),v_\pi(b)>0$.
Alors $\pi|a$ et $\pi|b$, or $\pi\notin A^*$. Donc a et b ne sont pas premiers entre eux. ■

Remarque 3.46. On a vu dans la démonstration que (2)⇔(3), (4)⇒(2) et (2)⇒(1) sont vrais sans supposer (E). L'hypothèse (E) a seulement été utilisée pour montrer que (1)⇒(4).

Proposition 3.47. *Si $(A,0,1,+,\cdot)$ est un anneau factoriel alors*

$$\forall \pi \in A,\ \pi \text{ est irréductible} \Leftrightarrow (\pi) \text{ est premier non nul.}$$

Démonstration. D'après la Proposition 3.31, pour tout anneau intègre, si (π) est un idéal premier non nul alors π est irréductible. La réciproque est vraie dans un anneau factoriel d'après 3.45.(3). ■

3.6 Divisibilité dans les anneaux principaux

Proposition 3.48. *Un anneau principal est factoriel.*

Démonstration. Soit $(A,0,1,+,\cdot)$ un anneau principal.
- A est intègre par définition, i.e. A vérifie (0).
- A est noethérien et vérifie donc (E), d'après la Proposition 3.35.
- Montrons que A vérifie 3.45.(3), et donc (U).
  Soit $\pi \in A$ un irréductible. On va montrer que (π) est maximal.
  - ⋆ Comme $\pi \notin A^*$, on déduit de la Proposition 2.27 que $(\pi) \neq A$.
  - ⋆ Soit I un idéal de A tel que $(\pi) \subset I$. Puisque A est principal, il existe $a \in A$ tel que $I = (a)$.
    Premier cas : $a \in A^*$. Alors $I = (a) = A$ d'après la Proposition 2.27.
    Deuxième cas : $a \notin A^*$. Alors $\pi \in (\pi) \subset I = (a)$. Donc il existe $b \in A$ tel que $\pi = ab$.
    Puisque π est irréductible et $a \notin A^*$, on a $b \in A^*$.
    Donc $I = (a) = (\pi)$ d'après la Proposition 2.27.

  Ainsi (π) est maximal et est donc premier. De plus $(\pi) \neq \{0\}$ puisque $\pi \neq 0$. ■

On sait qu'un anneau principal est factoriel, ainsi deux éléments d'un anneau principal admettent toujours un pgcd et un ppcm. On peut de plus les caractériser en termes de générateurs d'idéaux.

Proposition 3.49. *Soient $(A,0,1,+,\cdot)$ un anneau principal et $a,b \in A$.*
Alors a,b admettent un pgcd et un ppcm, de plus
(1) *$d \in A$ est un pgcd de a et b si et seulement si $(a)+(b)=(d)$,*
(2) *$m \in A$ est un ppcm de a et b si et seulement si $(a)\cap(b)=(m)$.*

Démonstration.

(1) Puisque A est principal, il existe $d \in A$ tel que $(a)+(b)=(d)$.
Montrons que d est un pgcd de a et b :
- $a \in (a) \subset (a)+(b)=(d)$ donc $d|a$.
- $b \in (b) \subset (a)+(b)=(d)$ donc $d|b$.
- Soit $c \in A$ tel que $c|a$ et $c|b$. Alors il existe $\alpha,\beta \in A$ tels que $a=\alpha c$ et $b=\beta c$.
  Puisque $d \in (d)=(a)+(b)$, il existe $u,v \in A$ tels que $d=au+bv$.
  Donc $d=au+bv=(\alpha u+\beta v)c$ et $c|d$.

Soit $d' \in A$.
Alors, d'après la Proposition 3.21, d' est un pgcd de a et b si et seulement si d et d' sont associés.
Donc, d'après la Proposition 3.13, d' est un pgcd de a et b si et seulement si $(d')=(d)=(a)+(b)$.

(2) Puisque A est principal, il existe $m \in A$ tel que $(a)\cap(b)=(m)$.
Montrons que m est un ppcm de a et b :
- $m \in (a)\cap(b) \subset (a)$ donc $a|m$.
- $m \in (a)\cap(b) \subset (b)$ donc $b|m$.
- Soit $c \in A$ tel que $a|c$ et $b|c$. Alors $c \in (a)\cap(b)=(m)$ donc $m|c$.

Soit $m' \in A$. Alors, d'après la Proposition 3.28, m' est un pgcd de a et b si et seulement si m et m' sont associés. Donc, d'après la Proposition 3.13, m' est un pgcd de a et b si et seulement si $(m')=(m)=(a)\cap(b)$. ■

Corollaire 3.50 (Relation de Bézout). *Soient $(A,0,1,+,\cdot)$ un anneau principal et $a,b,d \in A$.*
Si d est un pgcd de a et b alors il existe $u,v \in A$ tels que $d = au + bv$.

Démonstration. Supposons que d soit un pgcd de a et b. Alors, d'après la proposition précédente, $d \in (d) = (a) + (b)$. Donc il existe $u,v \in A$ tels que $d = au + bv$. ■

Corollaire 3.51 (Identité de Bézout). *Soient $(A,0,1,+,\cdot)$ un anneau principal et $a,b \in A$.*
Alors a et b sont premiers entre eux si et seulement s'il existe $u,v \in A$ tels que $1 = au + bv$.

Démonstration.

⇒ Supposons que a et b soient premiers entre eux et montrons que 1 est un pgcd de a et b.
On a $1|a$ et $1|b$. De plus si $c|a$ et $c|b$ alors $c \in A^*$ et donc $1|c$.
On déduit du corollaire précédent qu'il existe $u,v \in A$ tels que $1 = au + bv$.

⇐ Supposons qu'il existe $u,v \in A$ tels que $1 = au + bv$.
Soit $d \in A$ tel que $d|a$ et $d|b$ alors $d|au + bv = 1$ d'après la Proposition 3.4.
Il existe donc $u \in A$ tel que $1 = du$, i.e. $d \in A^*$.
Donc a et b sont premiers entre eux. ■

Proposition 3.52. *Tout idéal premier non nul d'un anneau principal est maximal.*

Démonstration. Soient $(A,0,1,+,\cdot)$ un anneau principal et $I \subset A$ un idéal premier non nul de A.
Puisque A est principal, il existe $x \in A$ tel que $I = (x)$. Comme $(x) \neq \{0\}$, on a $x \neq 0$.
Soit $J \subset A$ un idéal de A tel que $I \subset J$.
Puisque A est principal, il existe $y \in A$ tel que $J = (y)$.
Comme $x \in (x) = I \subset J = (y)$, il existe $z \in A$ tel que $x = yz$.
Ainsi $yz = x \in (x)$ et donc, puisque (x) est premier :

- Soit $y \in (x)$. Alors il existe $r \in A$ tel que $y = rx$. Ainsi $x(1 - rz) = x - rxz = x - yz = 0$.
  Donc, puisque $x \neq 0$ et que A est intègre, on a $rz = 1$.
  Par conséquent $z \in A^*$ et donc $J = (y) = (x) = I$ d'après la Proposition 2.27.
- Soit $z \in (x)$. Alors il existe $s \in A$ tel que $z = sx$. Ainsi $(1 - ys)x = x - ysx = x - yz = 0$.
  Donc, puisque $x \neq 0$ et que A est intègre, on a $ys = 1$.
  Par conséquent $y \in A^*$ et donc $J = A$ d'après la Proposition 2.27.

Donc I est maximal. ■

Corollaire 3.53. *Soient $(A,0,1,+,\cdot)$ un anneau principal et $\pi \in A \setminus \{0\}$.*
Alors les énoncés suivants sont équivalents :

(1) *(π) est maximal,*
(1′) *$A/(\pi)$ est un corps,*
(2) *(π) est premier,*
(2′) *$A/(\pi)$ est intègre,*
(3) *π est irréductible.*

Démonstration. On a :

- (1)⇔(1′) et (2)⇔(2′) d'après la Proposition 2.37.
- (1)⇒(2) d'après le Corollaire 2.38.
- (2)⇒(1) d'après la proposition précédente.
- D'après la Proposition 3.48, A est factoriel. Donc (2)⇔(3) d'après la Proposition 3.47. ■

3.7 Anneaux euclidiens

Définition 3.54. Un *anneau euclidien* est un anneau $(A,0,1,+,\cdot)$ intègre muni d'une fonction $\nu : A \setminus \{0\} \to \mathbb{N}$, appelée *stathme*, telle que

$$\forall a \in A,\ \forall b \in A \setminus \{0\},\ \exists q,r \in A,\ \begin{cases} a = bq + r \\ r = 0 \text{ ou } \nu(r) < \nu(b) \end{cases}$$

On dit alors que $a = bq + r$ est une *division de euclidienne* de a par b.

Remarque 3.55. Par convention, on prolonge ν en 0 par $\nu(0) := -\infty$.
Ainsi $\forall a \in A,\ a = 0 \Leftrightarrow \nu(a) = 0$ et la dernière condition de la définition peut simplement se réécrire $\nu(r) < \nu(b)$ (sans distinguer le cas $r = 0$).

Exemples 3.56.

- $\mathbb{Z}$ est un anneau euclidien pour $\nu := |\cdot|$.
- Un corps K est un anneau euclidien pour $\nu \equiv 1$.
- Si K est un corps alors $K[X]$ est un anneau euclidien pour $\nu := \deg$ (voir l'Exercice 1.8).
- $\mathbb{Z}[i]$ et $\mathbb{Z}\left[i\sqrt{2}\right]$ sont des anneaux euclidiens pour $\nu := |\cdot|^2$ (voir l'Exercice 3.10).
- $\mathbb{Z}\left[\sqrt{2}\right]$ est un anneau euclidien pour $\nu\left(a+b\sqrt{2}\right) := \left|a^2-2b^2\right|$ (voir l'Exercice 3.10).

Remarque 3.57. Il n'y a généralement pas unicité de la division euclidienne.
Par exemple, pour $4+5i$ et 3 dans $\mathbb{Z}[i]$ muni du stathme $\nu := |\cdot|^2$, on a

$$\begin{array}{lcll} 4+5i & = & 3(1+2i)+(1-i) & \nu(1-i)=2<9=\nu(3) \\ 4+5i & = & 3(2+2i)+(-2-i) & \nu(-2-i)=5<9=\nu(3) \\ 4+5i & = & 3(1+i)+(1+2i) & \nu(1+2i)=5<9=\nu(3) \\ 4+5i & = & 3(2+i)+(-2+2i) & \nu(1+2i)=8<9=\nu(3) \end{array}$$

Proposition 3.58. *Un anneau euclidien est principal.*

Démonstration. Soit $(A,0,1,+,\cdot)$ un anneau euclidien pour le stathme $\nu : A\setminus\{0\} \to \mathbb{N}$.
Soit I un idéal de A. Si $I = \{0\}$ alors $I = (0)$ est principal. On peut donc supposer que $I \neq \{0\}$.
Soit $b \in I\setminus\{0\}$ tel que $\nu(b)$ soit minimal.
Soit $a \in I$. Alors il existe $q, r \in A$ tels que $a = bq + r$ et soit $r = 0$ soit $\nu(r) < \nu(b)$.
Supposons par l'absurde que $r \neq 0$ avec $\nu(r) < \nu(b)$ alors $r = a - bq \in I$ mais $\nu(r) < \nu(b)$ ce qui contredit la minimalité de $\nu(b)$. Donc $r = 0$ et $a = bq \in (b)$.
Ainsi $I = (b)$ est principal. ■

Dans un anneau euclidien, l'algorithme d'Euclide permet de déterminer le pgcd de deux éléments.

Algorithme d'Euclide

Données : $(A,0,1,+,\cdot)$ un anneau euclidien pour le stathme $\nu : A\setminus\{0\} \to \mathbb{N}$
Entrées : $a, b \in A$
Résultat : un pgcd de a et b dans A
tant que $b \neq 0$ **faire**
  trouver $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\nu(r) < \nu(b)$
  $a \leftarrow b$
  $b \leftarrow r$
fin
retourner a

Lemme 3.59. *Soient $(A,0,1,+,\cdot)$ un anneau commutatif et $a, b, k, d \in A$.*
Alors d est un pgcd de a et b si et seulement si d est un pgcd de a et $b + ka$.

Démonstration.
⇒ Supposons que d soit un pgcd de a et b.
Alors $d|a$ et $d|b$. Donc $d|b + ka$ d'après la Proposition 3.4.
Soit $c \in A$ tel que $c|a$ et $c|b + ka$ alors $c|b = b + ka - ka$ d'après la Proposition 3.4.
Puisque d est un pgcd de a et b, on a $c|d$.
Donc d est un pgcd de a et $b + ka$.
⇐ Supposons que d soit un pgcd de a et $b + ka$.
Alors, d'après le point précédent, d est un pgcd de a et $b = b + ka - ka$. ■

Proposition 3.60. *L'algorithme d'Euclide termine en un nombre fini d'étapes et retourne un pgcd de a et b.*

Démonstration. Soient $a, b \in A$.
- Si $b = 0$ alors a est un pgcd de a et b d'après la Proposition 3.17.
- Si $b \neq 0$:
  - ⋆ Puisque A est supposé euclidien, il existe bien $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\nu(r) < \nu(b)$.
  - ⋆ D'après le lemme précédent d est un pgcd de a et b si et seulement si d est un pgcd de $r = a - bq$ et b.
  - ⋆ Si $r \neq 0$ alors $0 \leq \nu(r) < \nu(b)$ et donc l'algorithme termine après un nombre fini d'étapes. ■

Exemple 3.61. On cherche un pgcd de $4 + i$ et 3 dans $\mathbb{Z}[i]$ pour le stathme $\nu \equiv |\cdot|^2$:

$$\begin{array}{rcll} 4+i & = & 3\cdot 1 + (1+i) & \nu(1+i) = 2 < 9 = \nu(3) \\ 3 & = & (1+i)(1-i) + 1 & \nu(1) = 1 < 2 = \nu(1+i) \\ 1+i & = & 1\cdot(1+i) + 0 & \end{array}$$

Donc 1 est un pgcd de $4 + i$ et 3.

Puisque la division euclidienne n'est pas unique, l'algorithme peut donner d'autres pgcd :

$$\begin{array}{rcll} 4+i & = & 3\cdot 2 + (-2+i) & \nu(-2+i) = 5 < 9 = \nu(3) \\ 3 & = & (-2+i)(-1-i) + (-i) & \nu(-i) = 1 < 2 = \nu(-2+i) \\ -2+i & = & (-i)(-1+2i) + 0 & \end{array}$$

Donc $-i$ est un autre pgcd de $4 + i$ et 3.

Exemple 3.62. On cherche un pgcd de $12 + 45i$ et $4 + 12i$ dans $\mathbb{Z}[i]$ pour le stathme $\nu \equiv |\cdot|^2$:

$$\begin{array}{rcll} 12+45i & = & (4+12i)\cdot 4 + (-4-3i) & \nu(-4-3i) = 25 < 160 = \nu(2+12i) \\ 4+12i & = & (-4-3i)(-2-i) + (-1+2i) & \nu(-1+2i) = 5 < 25 = \nu(-4-3i) \\ -4-3i & = & (-1+2i)\cdot 2i + (-i) & \nu(-i) = 1 < 5 = \nu(-1+2i) \\ (-1+2i) & = & (-i)(-2-i) + 0 & \end{array}$$

Donc $-i$ est un pgcd de $12 + 45i$ et $4 + 12i$.

Exemple 3.63. On cherche un pgcd de $16 + 7i$ et $10 - 5i$ dans $\mathbb{Z}[i]$ pour le stathme $\nu \equiv |\cdot|^2$:

$$\begin{array}{rcll} 16+7i & = & (10-5i)(1+i) + (1+2i) & \nu(1+2i) = 5 < 125 = \nu(10-5i) \\ 10-5i & = & (1+2i)(-5i) + 0 & \end{array}$$

Donc $1 + 2i$ est un pgcd de $16 + 7i$ et $10 - 5i$.

3.8 Et les réciproques ?

On a vu qu'un anneau euclidien est principal et qu'un anneau principal est factoriel.
Les deux réciproques sont fausses.

Exemple 3.64. $\mathbb{Z}[X]$ est factoriel ***TODO*** mais n'est pas principal (voir l'Exercice 2.6).

Exemple 3.65. $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais n'est pas euclidien (voir l'Exercice 3.17).

Exercices

Exercice 3.1.

(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 3.2.

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 3.3.

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 3.4.

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 3.5.

(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 3.6.

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 3.7.
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 3.8.
On considère $A := \{P \in \mathbb{Q}[X] \ : \ P(0) \in \mathbb{Z}\}$.
(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 3.9. Soit $A := \{P \in \mathbb{Q}[X] \ : \ P'(0) = 0\}$.
(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 $I := (X^2, X^3)$ 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 3.10.
(1) Montrer que $\mathbb{Z}[i]$ est un anneau euclidien pour le stathme $\nu(z) := |z|^2$.
(2) Montrer que $\mathbb{Z}\left[\sqrt{2}\right]$ est un anneau euclidien pour le stathme $\nu\left(a + b\sqrt{2}\right) := \left|a^2 - 2b^2\right|$.

Exercice 3.11. 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 3.12. 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 3.13. 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 3.14 (Somme de deux carrés)**.**
Soient $A \coloneqq \mathbb{Z}[i]$ et $N : A \to \mathbb{N}$ défini par $N(z) \coloneqq |z|^2$.

(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 $\Sigma \coloneqq \left\{n \in \mathbb{N} \ :\ \exists a, b \in \mathbb{N},\ n = a^2 + b^2\right\}$ 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 3.15. Soit A un anneau intègre.

(1) Montrer que $\forall a, b \in A,\ \forall c \in A \setminus \{0\},\ a|b \Leftrightarrow ac|bc$.
(2) (a) Montrer que, pour tout $a \in A$, a est un pgcd de a et 0.
(b) Soit $(a, b) \in A^2 \setminus \{(0, 0)\}$. Montrer que si a et b admettent un pgcd alors il est non nul.
(3) Soient $(a, b) \in A^2 \setminus \{(0, 0)\}$ et d un pgcd de a et b.
(a) Montrer qu'il existe $a', b' \in A$ tels que $a = da'$ et $b = db'$.
(b) Montrer que a' et b' sont premiers entre eux.
(4) Soient $a, b, r \in A$ tels que ra et rb admettent un pgcd.
(a) Montrer que si $d \in A$ est un pgcd de a et b alors rd est un pgcd de ra et rb.
(b) Montrer que l'énoncé de la question précédente n'est plus vrai si on ne suppose pas que ra et rb admettent un pgcd.
Indice : on pourra montrer que 1 *est un pgcd de* 2 *et* $1 + i\sqrt{3}$ *dans* $\mathbb{Z}\left[i\sqrt{3}\right]$ *et conclure avec la Remarque 3.19.*
(5) Soient $a, b \in A$. L'objectif de cette question est de montrer que a et b ont un ppcm si et seulement si, pour tout $r \in A$, ra et rb ont un pgcd.
(a) On suppose que a et b ont un ppcm noté m. Soit $r \in A$.
i. Montrer qu'il existe $d \in A$ tel que $rab = md$.
ii. Montrer qu'un tel d est un pgcd de ra et rb.
(b) Réciproquement, on suppose que, pour tout $r \in A$, ra et rb ont un pgcd.
i. Soit d un pgcd de a et b. Montrer qu'il existe m tel que $ab = md$.
ii. Montrer que m est un ppcm de a et b.
(6) On suppose maintenant que A est un anneau intègre dont deux éléments quelconques ont toujours un pgcd.
L'objectif de cette question est de montrer que le lemme d'Euclide est vrai dans A.
(a) Soient $a, b, c \in A$ tels que
- a et b sont premiers entre eux,
- a et c sont premiers entre eux.

Montrer que a et bc sont premiers entre eux.
(b) Conclure.

Exercice 3.16.
L'objectif de cet exercice est de déterminer toutes les applications *surjectives* $f : \mathbb{Q}\setminus\{0\} \to \mathbb{Z}$ telles que
(i) $\forall x, y \in \mathbb{Q}\setminus\{0\},\ f(xy) = f(x) + f(y)$,
(ii) $\forall x, y \in \mathbb{Q}\setminus\{0\},\ f(x+y) \geq \min(f(x), f(y))$.
Pour tout l'exercice, on fixe une application f comme ci-dessus.

(1) (a) Montrer que $f(1) = f(-1) = 0$.
(b) Soit $x \in \mathbb{Q}\setminus\{0\}$. Montrer que $f(-x) = f(x)$ et que $f\left(x^{-1}\right) = -f(x)$.
(c) Montrer que si $n \in \mathbb{N}\setminus\{0\}$ alors $f(n) \geq 0$.
(d) En déduire que si $n \in \mathbb{Z}\setminus\{0\}$ alors $f(n) \geq 0$.

(2) On pose $A \coloneqq \{x \in \mathbb{Q}\setminus\{0\} \ :\ f(x) \geq 0\} \cup \{0\}$.
(a) Montrer que A est un sous-anneau de $\mathbb{Q}$ contenant $\mathbb{Z}$.
(b) Montrer que $A^* = \{x \in \mathbb{Q}\setminus\{0\} \ :\ f(x) = 0\}$,
i.e. que les inversibles de A sont les antécédents de 0 par f.

(3) (a) Montrer qu'il existe $\pi \in A$ tel que $f(\pi) = 1$.
(b) Montrer qu'un tel π est irréductible dans A.
(c) Montrer que si $\pi = \frac{a}{b}$ avec a et b premiers entre eux dans $\mathbb{Z}$ alors $f(a) = 1$ et $f(b) = 0$.
Indice : on pourra utiliser une relation de Bézout dans $\mathbb{Z}$.
(d) En déduire qu'il existe un nombre premier p tel que $f(p) = 1$.
On fixe un tel p dans la suite.

(4) Montrer que pour tout $n \in \mathbb{Z}$, si p ne divise pas n dans $\mathbb{Z}$ alors $f(n) = 0$.
Indice : on pourra utiliser une relation de Bézout dans $\mathbb{Z}$.

(5) Soit $x \in \mathbb{Q}\setminus\{0\}$.
(a) Montrer qu'il existe $a, b, n \in \mathbb{Z}$ tels que $x = \frac{a}{b}p^n$, $p \nmid a$ et $p \nmid b$.
(b) Déterminer $f(x)$ en fonction de n.

(6) Conclure : quelles sont les applications surjectives $f : \mathbb{Q}\setminus\{0\} \to \mathbb{Z}$ vérifiant (i) et (ii) ?

Les questions suivantes concernent l'étude de l'anneau A défini à la question (2).

(7) (a) Montrer que pour tout $x \in \mathbb{Q}\setminus\{0\}$, $x \in A$ ou $x^{-1} \in A$.
(b) En déduire que pour tout $x, y \in A\setminus\{0\}$, x divise y ou y divise x dans A.

(8) Soit I un idéal non-nul de A.
(a) Justifier qu'il existe $x \in I\setminus\{0\}$ minimisant $f(x)$.
(b) Montrer que $I = (x)$.
(c) L'anneau A est-il noethérien ? factoriel ?
(d) Montrer que $I = \left(p^n\right)$ où $n \coloneqq f(x) \in \mathbb{N}$.
(e) En déduire qu'il existe une bijection décroissante entre $\mathbb{N}$ et les idéaux non-nuls de A.

(9) Soit B un sous-anneau de $\mathbb{Q}$ contenant strictement A.
(a) Montrer que $\frac{1}{p} \in B$.
(b) En déduire que $B = \mathbb{Q}$.

Exercice 3.17.
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) $(\mathbb{R}, \nu \coloneqq 1)$ (2) $(\mathbb{Z}, \nu \coloneqq |\cdot|)$ (3) $(\mathbb{R}[X], \nu \coloneqq \deg)$ (4) $\left(\mathbb{Z}[i], \nu \coloneqq |\cdot|^2\right)$

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

(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 $N(z) \coloneqq z\overline{z}$.
  (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 3.18. Quel est le point commun entre un Nazgûl et un schéma affine ?