Université d'Angers – 2023/2024

Théorie des anneaux

CC du 04/04/2024.

Aucun document ou appareil électronique n'est autorisé.
Sauf mention contraire, vous devez ***justifier toutes vos réponses****.*
La note tiendra compte de la qualité et de la concision de la rédaction.
Vous pouvez utiliser tous les résultats du cours. Ces résultats doivent être cités correctement.

Exercice 1.

(1) Qu'est-ce qu'un anneau noethérien ?
(2) Déterminer les pgcd de $42+31i$ et $9+17i$ dans $\mathbb{Z}[i]$.
(3) a. Soient A un anneau intègre et $a \in A$.
Montrer que si (a) est un idéal premier non-nul alors a est irréductible.
b. On considère la réciproque : pour tout $a \in A$, si a est irréductible alors (a) est premier non-nul.
Cet énoncé est-il vrai pour les anneaux suivants ? Écrire vrai ou faux sans justifier.
i. A est un anneau intègre.
ii. A est un anneau euclidien.
iii. A est un anneau principal.
iv. A est un anneau factoriel.

Exercice 2.

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 de 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 de 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.

On suppose désormais que A est un anneau intègre dont deux éléments quelconques ont toujours un pgcd.
(4) Soient $a, b, r \in A$. Soit d un pgcd de a et de b. Montrer que rd est un pgcd de ra et de rb.
Indice : lorsque $r \neq 0$, on pourra montrer que si δ est un pgcd de ra et de rb alors δ et rd sont associés.
(5) Soit $(a,b) \in A^2 \setminus \{(0,0)\}$.
a. Soit d un pgcd de a et de b. Montrer qu'il existe $m \in A$ tel que $ab = md$.
b. Montrer que m est un ppcm de a et de b.
(6) 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.
(7) a. Rappeler l'énoncé du lemme d'Euclide.
b. Montrer que A vérifie le lemme d'Euclide.

Exercice 3.

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

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

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 $(a_1,b_1), (a_2,b_2), (c_1,d_1), (c_2,d_2) \in A \times (A \setminus \{0\})$,

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

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

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

Il n'est pas nécessaire de noter les indices $_K$ sur vos copies lorsqu'il n'y a pas de confusion possible.

a. Montrer que $\forall a \in A$, $\forall b, c \in A \smallsetminus \{0\}$, $\dfrac{ac}{bc} = \dfrac{a}{b}$.
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 $\tilde{\varphi}\left(\frac{a}{b}\right) \coloneqq \varphi(a)\varphi(b)^{-1}$.

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 $\mathbb{Z}$.

Solution de l'exercice 1.

(1) Un anneau noethérien est un anneau commutatif vérifiant les propriétés équivalentes suivantes :
- Tout idéal est finiment engendré.
- Toute suite croissante (pour l'inclusion) d'idéaux est stationnaire.
- Tout ensemble non-vide d'idéaux admet un élément maximal (pour l'inclusion).

Il suffisait de donner une des propriétés précédentes pour avoir tous les points.

(2) On utilise l'algorithme d'Euclide dans $\mathbb{Z}[i]$ pour le stathme $N(z) = |z|^2$:

$$\begin{array}{ll} (42+31i) = (9+17i)(2-i) + (7+6i) & N(7+6i) = 85 < 370 = N(9+17i) \\ (9+17i) = (7+6i)(2+i) + (1-2i) & N(1-2i) = 5 < 85 = N(7+6i) \\ (7+6i) = (1-2i)(4i-1) + 0 & \end{array}$$

Donc un pgcd de $42+31i$ et $9+17i$ est $1-2i$.
On sait que le pgcd est unique à association près et que $A^* = \{\pm 1, \pm i\}$.
Puisque A est intègre, on en déduit l'ensemble des pgcd de $42+31i$ et $9+17i$:

$$1-2i,\ -1+2i,\ 2+i,\ -2-i.$$

Remarque. Pour obtenir la première DE, il n'était pas nécessaire de faire des calculs exacts :

$$\begin{aligned} \frac{42+31i}{9+17i} = \frac{(42+31i)(9-17i)}{9^2+17^2} &= \frac{(42\times 9 + 31\times 17) + (31\times 9 - 17\times 42)i}{9^2+17^2} \\ &\simeq \frac{(40\times 10 + 30\times 20) + (30\times 10 - 20\times 40)}{10^2+20^2} = \frac{1000-500i}{500} = 2-i \end{aligned}$$

(3) a. Soit $a \in A$ tel que (a) soit un idéal premier non-nul.
- Puisque $(a) \neq \{0\}$, on a $a \neq 0$.
- Puisque $(a) \neq A$, car premier, on a $a \notin A^*$.
- Soient $b, c \in A$ tels que $a = bc$. Alors $bc = a \in (a)$.
  Donc, puisque (a) est premier, on a $b \in (a)$ ou $c \in (a)$.
  Sans perte de généralité, on peut supposer que $b \in (a)$. Alors il existe $\beta \in A$ tel que $b = a\beta$.
  Donc $0 = a - bc = a(1-\beta c)$ d'où $1 - \beta c = 0$ puisque A est intègre et que $a \neq 0$.
  Ainsi $\beta c = 1$ et c est donc inversible.

On a bien montré que a est irréductible.

b. i. Faux : dans $\mathbb{Z}\left[i\sqrt{3}\right]$, 2 est irréductible et $\left(1+i\sqrt{3}\right)\left(1-i\sqrt{3}\right) = 4 \in (2)$ mais $1 \pm i\sqrt{3} \notin (2)$.
ii. Vrai : un anneau euclidien est principal, voir point suivant.
iii. Vrai : un anneau principal est factoriel, voir point suivant.
iv. Vrai : c'est une caractérisation de l'unicité de la décomposition en irréductibles.

Solution de l'exercice 2.

(1) Soient $a, b \in A$ et $c \in A \setminus \{0\}$.
Supposons que $a|b$, alors il existe $x \in A$ tel que $b = ax$. D'où $bc = acx$. Ainsi $ac|bc$.
Supposons que $ac|bc$, alors il existe $y \in A$ tel que $bc = acy$. D'où $c(b - ay) = 0$. Puisque $c \neq 0$ et que A est intègre, on a que $b = ay$. Ainsi $a|b$.
On a bien montré que $a|b$ si et seulement si $ac|bc$.

(2) a. Soit $a \in A$. Alors $a|a$ 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 de 0.

b. Soit $(a, b) \in A^2 \setminus \{(0,0)\}$. Supposons que a et b admettent un pgcd noté d.
Supposons par l'absurde que $d = 0$. Alors, puisque $0|a$ et $0|b$, on a $a = b = 0$.
D'où une contradiction.

(3) a. Puisque $d|a$ et $d|b$, il existe $a', b' \in A$ tels que $a = da'$ et $b = db'$.
b. Soit $c \in A$ tel que $c|a'$ et $c|b'$. Alors $cd|a'd = a$ et $cd|b'd = b$.
Donc $cd|d$, d'où $c|1$ puisque d est non-nul (car $(a, b) \neq (0, 0)$). Ainsi $c \in A^*$.
On a bien montré que a' et b' sont premiers entre eux.

(4) *Premier cas :* si $r = 0$ alors $0 = rd$ est un pgcd de $ra = 0$ et de $rb = 0$.
Deuxième cas : supposons $r \neq 0$.
Soit δ un pgcd de ra et de rb.
On sait que $d|a$ et que $d|b$. Alors $rd|ra$ et $rd|rb$. Ainsi $rd|\delta$.
Puisque $r|ra$ et $r|rb$, on a $r|\delta$. Il existe donc $s \in A$ tel que $\delta = rs$. Donc $rs|ra$ d'où $s|a$ car $r \neq 0$.
De même $s|b$.
Puisque $s|a$ et $s|b$, on a que $s|d$ d'où $\delta = rs|rd$.
Ainsi $rd|\delta$ et $\delta|rd$ donc rd et δ sont associés.
Puisque δ est un pgcd de ra et de rb, on en déduit que δ aussi.

Remarque : *dans un anneau intègre quelconque, il n'est pas vrai en général que si d est un pgcd de a et de b alors rd est un pgcd de ra et de rb. L'hypothèse que ra et rb admettent un pgcd est nécessaire.*
Dans $A = \mathbb{Z}\left[i\sqrt{3}\right]$: 1 est un pgcd 2 et $1 + i\sqrt{3}$ mais $2 = 2 \times 1$ n'est pas un pgcd de 4 et de $2\left(1 + i\sqrt{3}\right)$ (on a vu en cours qu'ils n'avaient pas de pgcd).

(5) a. On a que $d|a$ et que $a|ab$, donc $d|ab$. Ainsi il existe $m \in A$ tel que $ab = md$.
b.
- *Premier cas :* si $a = 0$ alors $md = ab = 0$ et donc $m = 0$ puisque $d \neq 0$. D'où $b|m$.
Deuxième cas : si $a \neq 0$ alors, puisque $d|a$, on a $ab = md|ma$ d'où $b|m$.
- On montre de même que $a|m$.
- Soit $c \in A$ tel que $a|c$ et $b|c$. Alors $ab|bc$ et $ab|ac$. Ainsi, puisque cd est un pgcd de ac et de bc d'après la question 4, ab divise cd. Donc $md = ab|cd$. D'où $m|c$ puisque $d \neq 0$.

(6) Soient $a, b, c \in A$ tels que a et b sont premiers entre eux, et a et c sont premiers entre eux.
Soit $d \in A$ tel que $d|a$ et $d|bc$.
Alors $d|ab$ et $d|bc$. Puisque 1 est un pgcd de a et de b, on déduit de la question 4 que $b = b \cdot 1$ est un pgcd de ab et de bc. Ainsi $d|b$.
Puisque $d|a$ et $d|b$, et que a et b sont premiers entre eux, on a que d est inversible.
Donc a et bc sont premiers entre eux.

(7) a. Lemme d'Euclide : soient $a, b, c \in A$ tels que $a|bc$ et a soit irréductible alors $a|b$ ou $a|c$.

b. Soit $a \in A$ un élément irréductible.
On remarque qu'étant donné $x \in A$, soit a divise x soit a et x sont premiers entre eux : en effet, si $d \in A$ est un diviseur commun à a et x, alors, puisque a est irréductible, soit d est inversible, soit d est associé à a (et donc a divise x).
Le lemme d'Euclide est donc la contraposée de l'énoncé de la question 6.

Solution de l'exercice 3.

(1)
- *Réflexivité.* Soit $(a, b) \in A \times (A \setminus \{0\})$ alors $ab - ba = 0$ et donc $(a, b) \sim (a, b)$.
- *Symétrie.* Soient $(a, b), (c, d) \in A \times (A \setminus \{0\})$ tels que $(a, b) \sim (c, d)$, alors $cb - da = -(ad - bc) = 0$, donc $(c, d) \sim (a, b)$.
- *Transitivité.* Soient $(a, b), (c, d), (e, f) \in A \times (A \setminus \{0\})$ tels que $(a, b) \sim (c, d)$ et $(c, d) \sim (e, f)$, alors $d(af - be) = adf - bde = adf - bcf + bcf - bde = (ad - bc)f + b(cf - de) = 0$ et donc $af - be = 0$ puisque A est intègre et $d \neq 0$.

(2) a. Soient $(a, b), (c, d) \in A \times (A \setminus \{0\})$ alors $bd \neq 0$ puisque A est intègre. Donc les deux lois considérées sont bien définies.

b. Soient $(a_1,b_1),(a_2,b_2),(c_1,d_1),(c_2,d_2) \in A\times(A\smallsetminus\{0\})$ tels que $(a_1,b_1)\sim(a_2,b_2)$ et $(c_1,d_1)\sim(c_2,d_2)$. Alors

$$\begin{aligned}(a_1d_1+b_1c_1)b_2d_2-b_1d_1(a_2d_2+b_2c_2) &= a_1d_1b_2d_2+b_1c_1b_2d_2-b_1d_1a_2d_2-b_1d_1b_2c_2\\ &= (a_1b_2-b_1a_2)d_1d_2+(c_1d_2-d_1c_2)b_1b_2=0\end{aligned}$$

Donc $(a_1d_1+b_1c_1,b_1d_1)\sim(a_2d_2+b_2c_2,b_2d_2)$, i.e. $(a_1,b_1)+(c_1,d_1)\sim(a_2,b_2)+(c_2,d_2)$.
De même,

$$\begin{aligned}a_1c_1b_2d_2-a_2c_2b_1d_1 &= a_1c_1b_2d_2-a_2b_1c_1d_2+a_2b_1c_1d_2-a_2c_2b_1d_1\\ &=(a_1b_2-b_1a_2)c_1d_2+(c_1d_2-c_2d_1)a_2b_1=0\end{aligned}$$

Donc $(a_1c_1,b_1d_1)\sim(a_2c_2,b_2d_2)$, i.e. $(a_1,b_1)\cdot(c_1,d_1)\sim(a_2,b_2)\cdot(c_2,d_2)$.

(3) a. Soient $a\in A$ et $b,c\in A\smallsetminus\{0\}$ alors $(ac)b-(bc)a=0$, donc $\frac{ac}{bc}=\frac{a}{b}$.

b. Montrons que $(K,+_K,\cdot_K,0_K,1_K)$ est un corps :

- $+_K$ est associative : soient $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in K$ alors

$$\begin{aligned}\left(\frac{a}{b}+_K\frac{c}{d}\right)+_K\frac{e}{f}=\frac{ad+bc}{bd}+_K\frac{e}{f}&=\frac{abf+bcf+bde}{bdf}\\ &=\frac{abf}{bdf}+_K\frac{bcf+ebd}{bdf}=\frac{a}{b}+_K\frac{cf+ed}{df}=\frac{a}{b}+_K\left(\frac{c}{d}+_K\frac{e}{f}\right).\end{aligned}$$

- $+_K$ est commutative : soient $\frac{a}{b},\frac{c}{d}\in K$ alors $\frac{a}{b}+_K\frac{c}{d}=\frac{ad+bc}{bd}=\frac{cb+da}{db}=\frac{c}{d}+_K\frac{a}{b}$.
- 0_K est le neutre de $+_K$: soit $\frac{a}{b}\in K$ alors $\frac{a}{b}+_K 0_K=\frac{a}{b}+_K\frac{0}{1}=\frac{a\cdot 1+b\cdot 0}{b\cdot 1}=\frac{a}{b}$.
- Tout élément admet un inverse additif : soit $\frac{a}{b}\in K$ alors $\frac{a}{b}+_K\frac{-a}{b}=\frac{ab+b(-a)}{b}=\frac{0}{b}=0_K$.
- $\cdot_K$ est associative : soient $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in K$ alors

$$\left(\frac{a}{b}\cdot_K\frac{c}{d}\right)\cdot_K\frac{e}{f}=\frac{ac}{bd}\cdot_K\frac{e}{f}=\frac{ace}{bdf}=\frac{a}{b}\cdot_K\frac{ce}{df}=\frac{a}{b}\cdot_K\left(\frac{c}{d}\cdot_K\frac{e}{f}\right).$$

- $\cdot_K$ est commutative : soient $\frac{a}{b},\frac{c}{d}\in K$ alors $\frac{a}{b}\cdot_K\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}\cdot_K\frac{a}{b}$.
- 1_K est le neutre de $\cdot_K$: soit $\frac{a}{b}\in K$ alors $\frac{a}{b}\cdot_K 1_K=\frac{a}{b}\cdot_K\frac{1}{1}=\frac{a\cdot 1}{b\cdot 1}=\frac{a}{b}$.
- $\cdot_K$ est distributive par rapport à $+_K$: soient $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in K$ alors

$$\frac{a}{b}\cdot_K\left(\frac{c}{d}+_K\frac{e}{f}\right)=\frac{a}{b}\cdot_K\frac{cf+de}{df}=\frac{acf+ade}{bdf}$$

et

$$\frac{a}{b}\cdot_K\frac{c}{d}+_K\frac{a}{b}\cdot_K\frac{e}{f}=\frac{ac}{bd}+_K\frac{ae}{bf}=\frac{acbf+bdae}{b^2df}=\frac{acf+ade}{bdf}$$

- Tout élément non-nul admet un inverse multiplicatif : soit $\frac{a}{b}\in K\smallsetminus\{0_K\}$ alors $a\neq 0$ et $\frac{b}{a}\in K$, puis

$$\frac{a}{b}\cdot_K\frac{b}{a}=\frac{ab}{ba}=\frac{1}{1}=1_K$$

(4)
- $\iota(1)=\frac{1}{1}=1_K$
- Soient $a,b\in A$ alors $\iota(ab)=\frac{ab}{1}=\frac{ab}{1\cdot 1}=\frac{a}{1}\cdot\frac{b}{1}=\varphi(a)\varphi(b)$
- Soient $a,b\in A$ alors $\iota(a+b)=\frac{a+b}{1}=\frac{a\cdot 1+1\cdot b}{1\cdot 1}=\frac{a}{1}+\frac{b}{1}=\varphi(a)+\varphi(b)$

Donc ι est un morphisme d'anneaux.

Montrons que ι est injectif.
Soit $a\in\ker(\iota)$ alors $\frac{0}{1}=0_K=\iota(a)=\frac{a}{1}$, i.e. $0=a\cdot 1-1\cdot 0=a$.
Donc $\ker(\iota)=\{0\}$ et ι est injectif.

(5) a. Soient $(a,b),(c,d) \in A \times (A \setminus \{0\})$ tels que $\frac{a}{b} = \frac{c}{d}$ alors $ad - bc = 0$, i.e. $ad = bc$.
Donc $\varphi(a)\varphi(d) = \varphi(ad) = \varphi(bc) = \varphi(b)\varphi(c)$.
En multipliant par $\varphi(b)^{-1}\varphi(d)^{-1}$, il vient $\varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1}$.
Donc $\tilde{\varphi}\left(\frac{a}{b}\right) = \tilde{\varphi}\left(\frac{c}{d}\right)$.

b.
- $\tilde{\varphi}(1_K)\tilde{\varphi}\left(\frac{1}{1}\right) = \varphi(1)\varphi(1)^{-1} = 1 \cdot 1^{-1} = 1$
- Soient $\frac{a}{b}, \frac{c}{d} \in K$ alors

$$\begin{aligned}\tilde{\varphi}\left(\frac{a}{b}\cdot\frac{c}{d}\right) = \tilde{\varphi}\left(\frac{ac}{bd}\right) &= \varphi(ac)\varphi(bd)^{-1}\\ &= \varphi(a)\varphi(c)\left(\varphi(b)\varphi(d)\right)^{-1} = \varphi(a)\varphi(b)^{-1}\varphi(c)\varphi(d)^{-1} = \tilde{\varphi}\left(\frac{a}{b}\right)\tilde{\varphi}\left(\frac{c}{d}\right)\end{aligned}$$

- Soient $\frac{a}{b}, \frac{c}{d} \in K$ alors

$$\begin{aligned}\tilde{\varphi}\left(\frac{a}{b}+\frac{c}{d}\right) = \tilde{\varphi}\left(\frac{ad+bc}{bd}\right) &= \varphi(ad+bc)\left(\varphi(bd)\right)^{-1}\\ &= \left(\varphi(a)\varphi(d)+\varphi(b)\varphi(c)\right)\left(\varphi(b)\varphi(d)\right)^{-1}\\ &= \left(\varphi(a)\varphi(d)+\varphi(b)\varphi(c)\right)\varphi(d)^{-1}\varphi(b)^{-1}\\ &= \varphi(a)\varphi(b)^{-1}+\varphi(c)\varphi(d)^{-1}\\ &= \tilde{\varphi}\left(\frac{a}{b}\right)+\tilde{\varphi}\left(\frac{c}{d}\right)\end{aligned}$$

Donc $\tilde{\varphi}$ est un morphisme d'anneaux.
C'est nécessairement un morphisme injectif puisqu'il est défini sur un corps.

c. Soit $\psi : K \to L$ vérifiant $\varphi = \psi \circ \imath$. Soient $a, b \in A \times (A \setminus \{0\})$, alors

$$\psi\left(\frac{a}{b}\right) = \psi\left(\frac{a}{1}\cdot\left(\frac{b}{1}\right)^{-1}\right) = \psi\left(\frac{a}{1}\right)\psi\left(\frac{b}{1}\right)^{-1} = \psi(\imath(a))\psi(\imath(b))^{-1} = \varphi(a)\varphi(b)^{-1} = \tilde{\varphi}\left(\frac{a}{b}\right).$$

Donc $\psi = \tilde{\varphi}$.

(6) Le corps des fractions de $\mathbb{Z}$ est $\mathbb{Q}$ (à isomorphisme près).