EPFL - Printemps 2025	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 6	

Exercice 1. 1. Soit A un anneau Euclidien. Prouvez que l'algorithme d'Euclide peut être adapté pour calculer les pgdc dans A.

2. Effectuez la division avec reste de $27-23i$ par $8+i$ dans $\mathbb{Z}[i]$, et montrez que ces deux entiers de Gauss sont premiers entre eux.

3. Calculez un pgdc de $11+3i$ et de $1+8i$ dans $\mathbb{Z}[i]$. Ce pgdc est-il unique ?

4. Écrivez les idéaux $(11+3i)$ et de $(1+8i)$ comme un produit d'idéaux premiers de $\mathbb{Z}[i]$.

Solution.

1. Soit A un anneau euclidien, avec une fonction euclidienne $\nu\colon A\setminus\{0\}\to\mathbb{N}$. Etant donnés $a_0\in A$ et $0\neq a_1\in A$, on construit une suite d'éléments $a_i\in A$ de la manière récursive suivante :

   (a) a_0, a_1 sont donnés ;

   (b) pour $i\geq 1$, si $a_i\neq 0$, il existe une expression $a_{i-1}=a_iq_i+a_{i+1}$ où $\nu(a_{i+1})<\nu(a_i)$.

   La condition $\nu(a_{i+1})<\nu(a_i)$ implique que l'algorithme s'arrête, c'est-à-dire qu'il existe un n tel que $a_{n+1}=0$. On prétend que

   $$a_n \text{ est un pgdc de } a_0 \text{ et } a_1.$$

   Prouvons cette assertion. On prétend d'abord que a_n divise tous les a_i ($i\leq n$). On procède par induction descendante sur i. Puisque $a_{n+1}=0$, on a $a_n|a_{n-1}$. Si a_n divise $a_i,\dots,a_n$, alors comme

   $$a_{i-1}=a_iq_i+a_{i+1}$$

   on voit que a_n divise a_{i-1}.

   On prétend ensuite que si b divise a_0 et a_1, alors b divise a_n. En effet, comme $a_2=a_0-a_1q_1$, on voit que b divise a_2 ; et par induction croissante sur i, on voit que b divise tous les a_i, en particulier a_n.

   La combinaison de ces deux observations montre que a_n est un pgdc de a_0 et de a_1.

   Faisons la remarque suivante, qui sera utile dans la suite : si une étape de l'algorithme fournit une unité, c'est-à-dire si $a_i\in A^\times$ pour un certain i, alors a_0 et a_1 sont premiers entre eux. En effet, puisque a_i est une unité, l'étape suivante sera

   $$a_{i-1}=(a_{i-1}a_i^{-1})a_i+0$$

   donc $a_{i+1}=0$ et ainsi a_i est un pgdc de a_0 et a_1. Par définition cela implique que a_0 et a_1 sont premiers entre eux.

2. La division de $27-23i$ par $8+i$ donne $\dfrac{193}{65}-\dfrac{211}{65}i$. On arrondit au nombre entier le plus proche pour trouver $q=3-3i$. Attention: on ne peut pas arrondir indifféremment vers le haut ou vers le bas, sans quoi le reste de la division aura une norme trop grande! On calcule alors

   $$27-23i=(3-3i)(8+i)+(-2i)$$

Le reste vaut donc $-2i$. On poursuit la recherche du pgdc avec l'algorithme d'Euclide dans cet anneau euclidien. Comme

$$8 + i = -4i^2 + i = 4i \cdot (-2i) + i$$

Le reste de cette division est i, un élément inversible de $\mathbb{Z}[i]$. On conclut que ces deux nombres sont premiers entre eux.

3. On calcule $11 + 3i = (1 - i)(1 + 8i) + 2 - 4i$. La division suivante $\dfrac{1 + 8i}{2 - 4i} = \dfrac{(1 + 8i)(2 + 4i)}{20} = \dfrac{-3 + 2i}{2}$ et nous retrouvons la possibilité de choisir deux quotients distincts: $q = -1 + i$ ou $q' = -2 + i$. Les restes correspondants sont $r = -1 + 2i$ et $r' = 1 - 2i$ respectivement. Dans les deux cas on constate que $2 - 4i$ est un multiple de ce reste.

   Ainsi le dernier reste non nul dans l'algorithme d'Euclide est $-1 + 2i$ ou $1 - 2i$. Chacun est un pgdc (de norme 5). Plus généralement, le pgdc est uniquement défini dans un anneau factoriel modulo la relation d'être associé.

4. Pour décomposer les idéaux premiers $(11 + 3i)$ et $(1 + 8i)$ on commence par décomposer leur normes dans les entiers.

$$(11 + 3i)(11 - 3i) = 130 = 13 \cdot 5 \cdot 2 \quad (1 + 8i)(1 - 8i) = 65 = 13 \cdot 5.$$

   Ensuite on décompose dans $\mathbb{Z}[i]$

$$13 = (3 + 2i)(3 - 2i) \quad 5 = (1 + 2i)(1 - 2i) \quad 2 = (1 + i)(1 - i).$$

   Notez que la décomposition de 2 en termes de multiplication d'idéaux est

$$(2) = (1 + i)^2.$$

   Notons que comme les éléments dans les décompositions ont norme première, ils sont forcément irréductibles, donc que leur idéal associé est un idéal premier (par factorialité de l'anneau.) Comme on sait déjà que $1 - 2i$ divise $1 + 8i$ on voit avec une division par $1 - 2i$ que c'est $3 - 2i$ qui divise également $1 + 8i$. En effet,

$$(2i - 3)(1 - 2i) = (-3 + 4) + i(6 + 2) = 1 + 8i.$$

   Ainsi, en termes de multiplication d'idéaux (noter qu'en termes d'idéaux la décomposition est unique)

$$(1 + 8i) = (3 - 2i)(1 - 2i).$$

   Comme on sait de plus que le pgcd de $11 + 3i$ et $1 + 8i$ est $1 - 2i$ on conclut que

$$(11 + 3i) = (3 + 2i)(1 - 2i)(1 + i).$$

Exercice 2.
Notons $\mathcal{C} := C^0([0, 1]; \mathbb{R})$ l'anneau des fonctions réelles continues sur l'intervalle $[0, 1]$ (muni des opérations d'addition et de multiplication de fonctions).

1. Pour $x \in [0, 1]$, écrivons $I_x := \{f \in \mathcal{C} \mid f(x) = 0\}$. Montrez que I_x est un idéal maximal.
2. Pour $x \neq y$, montrez que $I_x \cap I_y$ n'est pas un idéal premier.
3. Soit $I \subset \mathcal{C}$ un idéal. Supposons que I n'est contenu dans aucun des I_x. Montrez que $I = \mathcal{C}$. *Indication : la propriété de Heine–Borel sera utile.*

4. Montrez que tout idéal maximal de $\mathcal{C}$ est égal à I_x pour un certain $x \in [0,1]$.

Solution.

1. Pour $x \in [0,1]$, considérons l'application d'évaluation

$$\mathrm{ev}_x \colon \mathcal{C} \to \mathbb{R}, \quad f \mapsto f(x).$$

Alors ev_x est surjective et $\ker \mathrm{ev}_x = I_x$. Donc $\mathcal{C}/I_x \cong \mathbb{R}$ par le premier théorème d'isomorphisme, et ainsi I_x est maximal puisque $\mathbb{R}$ est un corps.

2. Il est facile de trouver $f, g \in \mathcal{C}$ tels que $f(x) = 0 = g(y)$ et $f(y) \neq 0 \neq g(x)$ (on peut construire de telles fonctions linéaires par parties). Donc ni f ni g n'appartient à $I_x \cap I_y = \{h \in \mathcal{C} \mid h(x) = 0 = h(y)\}$, tandis que $fg \in I_x \cap I_y$.

3. Pour chaque $x \in [0,1]$, par hypothèse il existe $0 \neq f_x \in I$ tel que $f_x(x) \neq 0$. Puisque f_x est continue, l'ensemble $\mathcal{U}_x := \{y \in [0,1] \mid f_x(y) \neq 0\}$ est ouvert (dans la topologie euclidienne de $[0,1]$) et contient x. Ainsi

$$[0,1] = \bigcup_{x \in [0,1]} \mathcal{U}_x.$$

Puisque la topologie euclidienne fait de $[0,1]$ un espace compact, la propriété de Heine–Borel implique qu'il existe $x_1, \ldots, x_n \in [0,1]$ tels que

$$[0,1] = \bigcup_{i=1}^{n} \mathcal{U}_{x_i}.$$

Considérons maintenant la fonction continue

$$F := \sum_{i=1}^{n} f_{x_i}^2.$$

Alors $F \in I$ et par construction F est strictement positive sur $[0,1]$. Ainsi $1/F \in \mathcal{C}$, et $1 = F \cdot 1/F \in I$. Donc $I = \mathcal{C}$.

4. Soit $I \subset \mathcal{C}$ un idéal maximal. En vertu du point précédent, puisque $I \neq \mathcal{C}$ il existe un I_x tel que $I \subseteq I_x$. Puisque I est maximal, on en déduit que $I = I_x$.

Il est également possible de définir une topologie sur l'ensemble $\{I_x \mid x \in [0,1]\}$ (la topologie la moins fine pour laquelle les sous-ensembles $\{I_x \mid f \in I_x\}$ sont ouverts pour des $f \in \mathcal{C}$ quelconques), pour laquelle la bijection

$$[0;1] \to \{\text{idéaux maximaux de } \mathcal{C}\}, \quad x \mapsto I_x$$

devient un homéomorphisme. En d'autres termes, il est possible de reconstruire l'espace topologique $[0,1]$ à partir de son anneau de fonctions réelles continues. C'est une forme de *dualité* entre $[0,1]$ et $\mathcal{C}$. Le même résultat est vrai plus généralement pour les espaces topologiques Hausdorff et compacts, cela s'appelle la "Gelfand-Kolomogorov duality".

Exercice 3.
Considérons les polynômes $f = x^3 - 2x^2 + x - 2$ et $g = x^4 - 2x^3 + 7x - 14$ dans $\mathbb{Z}[x]$.

1. Montrez que le pgdc de f et de g dans $\mathbb{Z}[x]$ vaut $x-2$ en écrivant $f = (x-2)f_0$ et $g = (x-2)g_0$ dans $\mathbb{Z}[x]$.

2. Pour un premier p, notons $\bar{f}$ et $\bar{g}$ la réduction de f et g dans $\mathbb{F}_p[x]$. Calculez le pgdc de $\bar{f}$ et de $\bar{g}$ pour chaque p.
Indication : Remarquez que les étapes de l'algorithme d'Euclide définissables dans $\mathbb{Z}[x]$ sont des étapes de l'algorithme d'Euclide dans $\mathbb{F}_p[x]$ après réduction modulo p.

Solution.

1. On vérifie que
$$f(x) = (x-2)(x^2+1) \quad \text{et} \quad g(x) = (x-2)(x^3+7),$$
et on prétend que x^2+1 et x^3+7 sont premiers entre eux. En fait, ces deux polynômes sont primitifs et ne se décomposent pas dans $\mathbb{Q}[x]$ (car -1 n'as pas de racine carrée dans $\mathbb{Q}$, et -7 n'a pas de racine cubique dans $\mathbb{Q}$), et donc ils sont irréductibles en vertu du lemme de Gauss III. Ainsi $x-2$ est un pgdc de f et de g.

2. Les décompositions $f = (x-2)(x^2+1)$ et $g = (x-2)(x^3+7)$ sont encore valables après la réduction modulo p. Après cette réduction, le pgdc n'est plus égal à $x - [2]_p$ si et seulement si $x^2 + [1]_p$ et $x^3 + [7]_p$ ne sont plus premiers entre eux dans $\mathbb{F}_p[x]$.

   Notons qu'on peut écrire (en suivant la méthode de l'algorithme d'Euclide, même si $\mathbb{Z}[x]$ n'est pas euclidien) :
$$x^3 + 7 = x(x^2+1) + (-x+7), \quad x^2 + 1 = (-x-7)(-x+7) + 50$$
et ces égalités sont encore valables modulo p. En fait, comme $\mathbb{F}_p[x]$ est un anneau euclidien dont la fonction euclidienne est donnée par le degré, la réduction modulo p de ces deux égalités donne les deux premiers pas de l'algorithme d'Euclide pour $x^3+[7]_p$ et $x^2+[1]_p$ (voir l'Exercice 1.1). Notons que le second reste est $[50]_p$. Si $[50]_p = 0$, alors l'algorithme est complet et
$$\operatorname{pgdc}(x^2 + [1]_p, x^3 + [7]_p) = -x + [7]_p \quad \text{et ainsi} \quad \operatorname{pgdc}(\bar{f}, \bar{g}) = (x - [2]_p)(-x + [7]_p).$$
   Si $[50]_p \neq 0$, alors il s'agit d'une unité dans $\mathbb{F}_p[x]$, et donc la prochaine étape de l'algorithme donne un reste nul. Ainsi le pgdc de $x^2 + [1]_p$ et de $x^3 + [7]_p$ est une unité, autrement dit ces deux polynômes sont encore premiers entre eux.

   Puisque $50 = 2 \cdot 5^2$, on a $[50]_p = 0$ si et seulement si $p \in \{2, 5\}$. Ainsi :

   (a) Si $p \notin \{2, 5\}$, alors $\operatorname{pgdc}(\bar{f}, \bar{g}) = x - [2]_p$.
   (b) Si $p = 2$, alors $\operatorname{pgdc}(\bar{f}, \bar{g}) = x(x + [1]_2)$.
   (c) Si $p = 5$, alors $\operatorname{pgdc}(\bar{f}, \bar{g}) = (x - [2]_5)(-x + [2]_5)$.

Exercice 4. 1. Soit $d > 0$ un entier positif. Montrez que $\mathbb{Q}[i\sqrt{d}]$ est un corps de fractions de $\mathbb{Z}[i\sqrt{d}]$.

2. Montrez que $x^3 - 2i$ est irréductible dans $(\mathbb{Z}[i])[x]$.
Indication : Utilisez le lemme de Gauss, et gardez en tête qu'un élément de $\mathbb{Q}[i]$ peut s'écrire comme $\frac{a+bi}{n}$ avec $a, b, n \in \mathbb{Z}$.

Solution.

1. Montrons d'abord que $\mathbb{Q}[i\sqrt{d}]$ est un corps. Puisque $(i\sqrt{d})^2 \in \mathbb{Q}$, on voit que
$$\mathbb{Q}[i\sqrt{d}] = \{a + bi\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$
   Les inverses de ces éléments existent dans $\mathbb{C}$, où ils sont donnés par
$$(a + bi\sqrt{d})^{-1} = \frac{a - bi\sqrt{d}}{|a + bi\sqrt{d}|^2}, \quad \text{où } |a + bi\sqrt{d}|^2 = a^2 + b^2 d \in \mathbb{Q}.$$

Le côté droit appartient aussi à $\mathbb{Q}[i\sqrt{d}]$, on en déduit donc qu'il s'agit d'un corps.

On a l' inclusion évidente $\mathbb{Z}[i\sqrt{d}] \subset \mathbb{Q}[i\sqrt{d}]$. Pour chaque $a + bi\sqrt{d} \in \mathbb{Q}[i\sqrt{d}]$, on peut écrire

$$a + bi\sqrt{d} = \frac{a'}{n} + \frac{b'}{n} i\sqrt{d}$$

où n est le plus petit dénominateur commun de a et b, et $a', b' \in \mathbb{Z}$. Ainsi $\mathbb{Q}[i\sqrt{d}]$ est un corps de fractions pour $\mathbb{Z}[i\sqrt{d}]$.

2. Montrons que $x^3 - 2i$ est irréductible dans $\mathbb{Z}[i][x]$. Puisque le coefficient dominant est une unité, ce polynôme est primitif. En vertu du lemme de Gauss et du premier point, il est irréductible dans $\mathbb{Z}[i][x]$ si et seulement si il est irréductible dans $\mathbb{Q}[i][x]$. Si $x^3 - 2i$ se décompose dans $\mathbb{Q}[i][x]$, l'un des facteurs doit être un polynôme linéaire. Donc $x^3 - 2i$ est irréductible dans $\mathbb{Q}[i][x]$ si et seulement si il n'a pas de racines dans $\mathbb{Q}[i]$.

   Supposons que $2i$ possède une racine cubique dans $\mathbb{Q}[i]$. On peut écrire cette racine $\frac{a+bi}{n}$, avec $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On a alors

$$n^3 2i = (a + bi)^3$$

   et en prenant les modules au carré, on obtient

$$4n^6 = (a^2 + b^2)^3.$$

   C'est une égalité entre deux entiers, on peut donc compter les puissances de 2 dans chaque membre et s'apercevoir qu'elles n'ont pas le même reste modulo 3. C'est une contradiction. Ainsi $2i$ n'a pas de racine cubique dans $\mathbb{Q}[i]$.

   On a donc montré que $x^3 - 2i$ est irréductible dans $\mathbb{Z}[i][x]$.

   Remarque : Le critère d'Eisenstein ne peut être invoqué pour résoudre l'exercice. En effet la décomposition en facteurs irréductibles de $2i$ est

$$2i = (1 + i)^2,$$

   où $1 + i$ est irréductible, comme il est de norme 2.

Exercice 5.
Soit k un corps.

1. Montrez que le sous-anneau $k[t^2, t^3] \subset k[t]$ n'est pas factoriel.
2. De même, montrez que $k[t^2, t^5]$ et $k[t^3, t^7]$ ne sont pas factoriels.
3. Montrez que $k[x, y]/(x^2 - y^3)$ n'est pas factoriel.
   Indication : Montrez que cet anneau est isomorphe à l'un des anneaux considérés précédemment.

Solution.

1. Notons $A = k[t^2, t^3]$. Puisque $A \subset k[t]$, on a

$$A^\times \subseteq (k[t])^\times = k^\times$$

   et l'inclusion inverse étant claire, on obtient $A^\times = k^\times$. On prétend ensuite que t^2 et t^3 sont irréductibles dans A :

   (a) Si on peut écrire $t^2 = fg$ dans A, alors cette décomposition est aussi valable dans $k[t]$. Donc soit f ou g est une unité dans $k[t]$ et donc dans A, soit $\deg f = 1 = \deg g$. Or A ne contient aucun polynôme linéaire en t (observez que $A = k + t^2 \cdot k[t] + t^3 \cdot k[t]$, et que les éléments de $t^2 \cdot k[t]$ et de $t^3 \cdot k[t]$ n'ont pas de termes d'ordre 1). On voit donc que t^2 est irréductible dans A.

(b) Pour t^3, on procède de la même manière : les seules décompositions non-triviales dans $k[t]$ sont données par $t^3 = t \cdot t \cdot t = t \cdot t^2$, mais $t \notin A$.

On peut ainsi affirmer que

$$(t^2)^3 = (t^3)^2 \quad \text{dans } A,$$

et que t^2 et t^3 sont des éléments irréductibles non associés de A, puisqu'il n'existe pas de constante $\lambda \in k^\times$ telle que $\lambda t^2 = t^3$. Cela montre que A n'est pas factoriel.

2. On montre de la même manière que $k[t^2, t^5]$ et $k[t^3, t^7]$ ne sont pas factoriels.

3. On prétend que $k[x,y]/(x^2-y^3)$ est isomorphe à $k[t^2, t^3]$. En effet, considérons l'homomorphisme d'évaluation k-linéaire

$$\varphi\colon k[x,y] \to k[t^2,t^3], \quad x \mapsto t^3,\ y \mapsto t^2.$$

Alors φ est surjective et $k[x,y]/\ker\varphi \cong k[t^2,t^3]$. On prétend que $\ker\varphi = (x^2-y^3)$. L'inclusion $\supseteq$ est claire. Pour montrer l'inclusion inverse, prenons $f \in \ker\varphi$ et faisons l'observation suivante : il existe un polynôme $g \in k[x,y]$ tel que $\deg_x[f-(x^2-y^3)\cdot g] < 2$. En effet, puisque $f-(x^2-y^3)\cdot g \in \ker\varphi$, cela se montre aisément par induction sur $\deg_x$ pour les éléments de $\ker\varphi$. Si nous montrons que $f-(x^2-y^3)\cdot g \in (x^2-y^3)$, nous aurons établi l'inclusion désirée. Nous pouvons donc supposer que $\deg_x f < 2$, et nous allons en fait montrer que $f = 0$.

Si $\deg_x f = 0$, alors $f = \sum_i a_i y^i$ et $\varphi(f) = \sum_i a_i t^{2i}$. Il est alors clair que $\varphi(f) = 0$ si et seulement si $f = 0$.

Si $\deg_x f = 1$, alors on peut écrire

$$f = \sum_i a_i y^i + \sum_j b_j x y^j$$

et ainsi

$$\varphi(f) = \sum_i a_i t^{2i} + \sum_j b_j t^{3+2j}.$$

Les puissances de t dans la première somme sont paires, celles dans la seconde sont impaires : il n'y a donc pas de simplifications possibles entre ces deux sommes, et on en déduit que $\varphi(f) = 0$ si et seulement si $f = 0$.

On a donc montré que $k[x,y]/(x^2-y^3) \cong k[t^2,t^3]$, ce qui conclut.

On aurait aussi pu montrer montrer l'inclusion $\ker(\varphi) \subseteq (x^2+y^3)$ en utilisant le lemme suivant :

Lemme. *Soit A un anneau factoriel, B un anneau intègre et $A \to B$ un morphisme injectif d'anneau. Soit $b \in B$ tel que $\ker(ev_b)$ est non-nul. Alors $\ker(ev_b)$ est principal, généré par un élément irréductible. Plus encore, si $p(t)$ est irréductible et $p(t) \in \ker(ev_b)$, alors $\ker(ev_b) = (p(t))$.*

Preuve. On montre qu'il ne peut exister au plus qu'un unique élément irréductible (modulo la relation d'être associé) dans $\ker(ev_b)$. Si deux éléments irréductibles non-associés $p(t)$ et $q(t)$ sont dans $\ker(ev_b)$ alors on aurait un élément non-nul $a \in A$ et $m(t), g(t) \in A[t]$ tel que

$$p(t)m(t) + q(t)g(t) = a$$

en utilisant que $p(t)$ et $q(t)$ seraient premiers entre eux dans l'anneau $\mathrm{Frac}(A)[t]$. En utilisant que $A \to B$ est injectif et en évaluant en b on obtient $a = 0$, une contradiction.

Si on décompose un élément non-nul du noyau en produit d'irréductibles, comme B est intègre, on voit qu'au moins un des facteurs irréductibles est dans $\ker(ev_b)$. Ainsi on a montré

l'existence d'un élément irréductible dans le noyau. Comme c'est en fait le seul (modulo la relation d'être associé) on voit qu'en fait $\ker(ev_b) = (p(t))$. □

Ainsi en appliquant le lemme pour $A = k[y]$ et $B = k[t^2, t^3]$ et $y \mapsto t^2$, on voit qu'il suffit de démontrer que $x^2 + y^3$ est irréductible. Cela peut se montrer exactement comme en 7.2.

Exercice 6.
Considérons l'anneau de matrices

$$A := \left\{ \begin{pmatrix} n & x \\ 0 & y \end{pmatrix} \mid n \in \mathbb{Z},\ x, y \in \mathbb{Q} \right\}$$

ainsi que le sous-ensemble

$$I := \left\{ \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \mid x \in \mathbb{Q} \right\} \subset A.$$

1. Montrez que I est un idéal bilatère, que $A/I \cong \mathbb{Z} \times \mathbb{Q}$ et que A/I est Noethérien.
2. Montrez que I est un idéal à droite minimal (c'est-à-dire qu'il n'existe pas d'idéal à droite J tel que $0 \subsetneq J \subsetneq I$).
3. Montrez que A est Noethérien à droite.
   Indication : Etant donnée une chaîne croissante d'idéaux, considérez son image par l'application quotient $A \to A/I$.

Solution.

1. Rappelons que

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix}$$

   de quoi il s'ensuit immédiatement que la fonction

$$A \to \mathbb{Z} \times \mathbb{Q}, \quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$$

   est un homomorphisme surjectif dont le noyau est I.

   Montrons maintenant que l'anneau commutatif $\mathbb{Z} \times \mathbb{Q}$ est Noethérien. Soit $I \subset \mathbb{Z} \times \mathbb{Q}$ un idéal. Il est facile de vérifier que l'intersection $I' := I \cap (\{0\} \times \mathbb{Q})$ est un idéal de $\mathbb{Q}$ via l'identification évidente $\mathbb{Q} = \{0\} \times \mathbb{Q}$. Puisque $\mathbb{Q}$ est un corps, on a $I' = \{(0,0)\}$ ou $I' = \{0\} \times \mathbb{Q}$.

   (a) Supposons que $I' = \{(0,0)\}$. Alors tous les éléments de I sont de la forme $(x, 0)$. En effet, si $(x, y) \in I$, alors $(0, 1) \cdot (x, y) \in I$ et donc $(0, y) \in I'$, d'où $y = 0$.

   Dans ce cas, I s'identifie à un idéal de $\mathbb{Z}$ via l'identification évidente $\mathbb{Z} = \mathbb{Z} \times \{0\}$. L'anneau $\mathbb{Z}$ est principal puisqu'il est Euclidien, donc on en déduit que I est généré par un élément de la forme $(n, 0)$.

   (b) Supposons que $I' = \{0\} \times \mathbb{Q}$. Alors on prétend que $I = I'' \times \mathbb{Q}$ pour un idéal I'' de $\mathbb{Z}$. En effet, soit $(x, y) \in I$. Puisque $(0, z) \in I'$ pour tout $z \in \mathbb{Q}$, on voit que $(x, y) + (0, z) = (x, y + z) \in I$ pour tout $z \in \mathbb{Q}$. Puisque la translation par y dans $\mathbb{Q}$ est bijective, on en déduit que $(x, z) \in I$ pour tout $z \in \mathbb{Q}$. Cela prouve qu'on peut écrire $I = I'' \times \mathbb{Q}$ pour un certain sous-ensemble $I'' \subset \mathbb{Z}$. Puisque I est un idéal, on vérifie aisément que I'' doit être un idéal de $\mathbb{Z}$. Si $I'' = (n)$, alors I est généré par $(n, 1)$.

   On a montré que tous les idéaux de $\mathbb{Z} \times \mathbb{Q}$ étaient finiment générés (en fait, ils sont tous principaux), ce qui montre que cet anneau produit est Noethérien (et même principal).

2. Soit J un idéal à droite qui contient un élément de la forme

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \quad 0 \neq b \in \mathbb{Q}.$$

Le calcul au début du point précédent montre alors que J contient tous les éléments de la forme

$$\begin{pmatrix} 0 & bz \\ 0 & 0 \end{pmatrix}, \quad z \in \mathbb{Q}$$

et il s'ensuit que $J \supseteq I$. Cela montre que I est minimal comme idéal à droite.

Notons que I n'est pas minimal comme idéal à gauche, puisqu'il contient strictement le sous-idéal à gauche

$$\left\{ \begin{pmatrix} 0 & n \\ 0 & 0 \end{pmatrix} \mid n \in \mathbb{Z} \right\}.$$

3. Montrons finalement que A est Noethérien à droite. Soit

$$J_1 \subseteq J_2 \subseteq \dots$$

une suite croissante d'idéaux à droite. Alors chaque $J_k \cap I$ est un sous-idéal à droite de I. Par le point précédent, pour chaque k on a soit $J_k \cap I = I$, soit $J_k \cap I = 0$. Puisque la suite est croissante, ces intersections sont toujours les mêmes pour k assez grand. Quitte à oublier les premiers idéaux, on peut donc supposer que $J_k \cap I = 0$ pour *tous* les k, ou que $J_k \cap I = I$ pour *tous* les k.

Considérons l'application quotient $\pi \colon A \to A/I$. Puisque π est surjective, les ensembles images $\pi(J_k)$ sont tous des idéaux (à droite) de A/I (la vérification est aisée), et on obtient une suite croissante d'idéaux

$$\pi(J_1) \subseteq \pi(J_2) \subseteq \dots$$

dans A/I. Nous avons montré dans le premier point que A/I est Noethérien : donc $\pi(J_k) = \pi(J_{k+1})$ pour tous les k assez grands.

On prétend que $\pi(J_k) = \pi(J_{k+1})$ entraîne $J_k = J_{k+1}$. Si ce n'est pas le cas, on peut trouver $x \in J_{k+1} \setminus J_k$. Puisque $\pi(x) \in \pi(J_{k+1}) = \pi(J_k)$, il existe $x' \in J_k$ tel que $x - x' \in \ker \pi = I$.

(a) Si $J_{k+1} \cap I = 0$, puisque $x - x' \in J_{k+1} \cap I$ on obtient $x = x' \in J_k$, contradiction.

(b) Si $J_{k+1} \cap I = I$, alors par notre simplification initiale on a aussi $J_k \cap I = I$ et donc $I \subseteq J_k$. Alors $x - x' \in J_k$ et ainsi $x = x' + (x - x') \in J_k$, contradiction.

Ainsi $J_k = J_{k+1}$ pour tous les k assez grands, ce qui montre que la chaîne d'idéaux se stabilise. Ainsi A est Noethérien à droite.

Exercice 7 ($\star$).
Soit $A = \mathbb{Z}[i\sqrt{d}]$ pour un $d \geq 1$. Pour un $a+bi\sqrt{d} \in \mathbb{Z}[i\sqrt{d}]$ on pose la norme $N(a+bi\sqrt{d}) = a^2+db^2$

1. Soit $x \in A$ non-nul. Montrer que

$$|A/(x)| = N(x).$$

(C'est à dire que la cardinalité du quotient est égale à la norme de x.)

Remarquer que A est un groupe abélien libre de rang 2 et que le quotient $A/(x)$ est égal au quotient de A par l'image de l'application linéaire $\cdot x : A \to A$, et utiliser la forme normale de Smith pour conclure.

Dans les points 2. et 3., on considère (B, σ) un anneau euclidien quelconque qui n'est pas un corps.

2. Montrer que si $b \in B$ est non-nul tel que $\sigma(b) = 0$, alors b est inversible.

3. Montrer qu'il existe un $b \in B$ non-nul et non inversible tel que

$$|B/(b)| \leq |B^\times| + 1.$$

4. Montrer que si $d > 3$, alors A n'est pas Euclidien. (Il ne s'agit pas de montrer que N n'est pas une fonction Euclidienne pour A, mais qu'il n'en existe aucune.)

Solution.

1. Prenons $x = a + bi\sqrt{d} \in A$ non-nul. On prend $(1, i\sqrt{d})$ comme $\mathbb{Z}$-base de A. Dès-lors il suit que la matrice de $\cdot x$ dans cette base est

$$\begin{pmatrix} a & -db \\ b & a \end{pmatrix}.$$

Le déterminant de cette matrice qui est égal $a^2 + bd^2 = N(x)$. Par la forme normale de Smith, il existe des automorphismes de groupes abéliens $f, g : A \to A$ tel que $f \circ (\cdot x) \circ g$ est sous forme diagonale dans la base $(1, i\sqrt{d})$. Soit donc $\alpha_1, \alpha_2 \in \mathbb{Z}$ tel que la matrice soit de forme,

$$\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}.$$

avec donc $|\alpha_1\alpha_2| = N(x)$. Ainsi on peut identifier $A/(x)$ *en tant que groupe abélien* à

$$\mathbb{Z}/\alpha_1\mathbb{Z} \oplus \mathbb{Z}/\alpha_2\mathbb{Z}$$

ce qui conclut. (Noter que comme le déterminant est non nul α_1 et α_2 sont aussi non-nuls, et donc ces groupes sont finis, de cardinal $|\alpha_1\alpha_2|$.)

2. Comme b est supposé non-nul, on peut diviser 1 par b pour obtenir

$$1 = bq + r,$$

avec $\sigma(r) < 0$ ou $r = 0$. Cela force $r = 0$.

3. Soit b non-inversible de norme minimale (on a $\sigma(b) > 0$, car sinon b serait inversible par le point précédent). Soit $a \in B$, et soient $q, r \in B$ tels que

$$a = bq + r.$$

Par hypothèse sur b, on a $\sigma(r) = 0$, et donc r est inversible ou nul par le point précédent. Comme $a \equiv r$ modulo b, on conclut la preuve.

4. Supposons par l'absurde que A soit Euclidien. Soit dès lors un élément $x = a + bi\sqrt{d} \in A$ comme au point précédent. Avec la norme multiplicative $N : A \to \mathbb{N}$, on voit que les seuls inversibles de A sont 1 et -1. Dès lors, une combinaison deux deux points précédents donne,

$$1 < a^2 + b^2 d \leq 3.$$

Comme $d > 3$ on voit que $b = 0$. Comme 2 et 3 ne sont pas des carrés d'entiers, on aboutit à une contradiction.