Exercices Algèbre - Anneaux I

Tous les anneaux de cette feuille d'exercices sont supposés être commutatif sauf mention explicite du contraire.

EXERCICE 1. Montrer que tout anneau intègre fini est un corps.

SOLUTION. Soit A un anneau intègre fini. On doit montrer que tout élément non nul de A est inversible. Pour $a \in A$, $a \neq 0$, on considère l'application $\varphi_a : x \in A \mapsto ax \in A$ qui est un morphisme de groupes $(A, +)$ dans $(A, +)$. Comme A est intègre on voit facilement que φ_a est injectif, donc surjectif car A est fini ; il existe donc en particulier $a' \in A$ tel que $aa' = 1$. Comme A est supposé commutatif, on a bien montré que a était inversible.

EXERCICE 2. Soit A un anneau commutatif, et soit S une partie multiplicative de A, c'est-à-dire que S contient 1, et si $s, t \in S$, alors $st \in S$. On veut définir la *localisation* $S^{-1}A$ de A par rapport à S.

1. Montrer qu'on peut définir une relation d'équivalence sur $A \times S$ comme suit : (a, s) est équivalent à (b, t) s'il existe un $u \in S$ tel que $u(at - bs) = 0$. Soit $S^{-1}A$ l'ensemble des classes d'équivalences. On écrira $\frac{a}{s}$ pour désigner la classe d'équivalence de (a, s).
2. Montrer que $S^{-1}A$, muni des opérations $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ et $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$, est un anneau commutatif.
3. Montrer que si S contient 0, alors $S^{-1}A$ est un anneau trivial.
4. Montrer que l'application $f : A \to S^{-1}A$ définie par $a \mapsto \frac{a}{1}$ est un morphisme d'anneaux. Montrer que f est injectif si S ne contient pas de diviseurs de zéro.
5. Cas particulier : corps des fractions. Supposons que A est intègre, et que $S = A \setminus \{0\}$. Montrer que $S^{-1}A$ est un corps, appelé le *corps des fractions* de A.
6. Cas particulier : localisation en un idéal premier. Soit P un idéal premier de A. Montrer que $S = A \setminus P$ est une partie multiplicative de A. On écrit A_P pour désigner $S^{-1}A$ dans ce cas.
7. Cas particulier (suite) : Montrer que l'idéal engendré par l'image de P dans A_P est le seul idéal maximal de A_P.

SOLUTION.

1. Montrons que la relation $\sim$ sur $A \times S$ est réflexive, symétrique et transitive : $\forall a, , b, c \in A$, $\forall s, t, k \in S$:
   - $(a, s) \sim (a, s)$ car $as - as = 0$.
   - supposons $(a, s) \sim (b, t)$ alors il existe $u \in S$ tel que $u(at - bs) = 0$; donc $(-u)(bs - at) = 0$ et donc $u(bs - at) = 0$ ce qui implique que $(b, t) \sim (a, s)$.
   - si $(a, s) \sim (b, t)$ et $(b, t) \sim (c, k)$ alors $\exists u, v \in S$ tels que $u(at-bs) = 0$ et $v(bk-ct) = 0$. Donc $uvt(ak-sc) = 0$ et on a que $(a, s) \sim (c, k)$.
2. Montrons que la somme est bien définie : si $\frac{a}{s} = \frac{a'}{s'}$ et $\frac{b}{t} = \frac{b'}{t'}$ alors il existe $u, v \in S$ tels que $u(as' - a's) = 0$ et $v(bt' - b't) = 0$; on a donc que

$$uv\big((at + bs)s't' - (a't' + b's')st\big) = uvtt'(as' - a's) + uvss'(bt' - b't) = 0 \quad \text{et} \frac{at + bs}{st} = \frac{a't' + b's'}{s't'}.$$

   De même $\frac{ab}{st} = \frac{a'b'}{s't'}$, car

$$\begin{aligned} uv(abs't' - a'b'st) &= uv(abs't' - a'bst' + a'bst' - a'b'st) \\ &= uv\big((as' - a's)bt' + (bt' - b't)a's\big) = 0 \end{aligned}$$

   Les deux opérations sont donc bien définies. Montrons maintenant que $(S^{-1}A, +, .)$ est un anneau commutatif : soient $\frac{a}{s}, \frac{b}{t}, \frac{c}{u} \in S^{-1}A$,
   - $+$ est associative : $(\frac{a}{s} + \frac{b}{t}) + \frac{c}{u} = \frac{(at+bs)u+cst}{stu} = \frac{a}{s} + (\frac{b}{t} + \frac{c}{u})$,
   - $\frac{0}{1}$ est l'élément neutre pour $+$,
   - $\frac{-a}{s}$ est l'inverse de $\frac{a}{s}$,

— $(A,+)$ est commutative $\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st}=\frac{bs+at}{ts}=\frac{b}{t}+\frac{a}{s}$,

— la multiplication est associative : $(\frac{a}{s}.\frac{b}{t}).\frac{c}{u}=\frac{abc}{stu}=\frac{a}{s}.(\frac{b}{t}.\frac{c}{u})$

— la multiplication est distributive par rapport à l'addition : $\frac{a}{s}.(\frac{b}{t}+\frac{c}{u})=\frac{abu+act}{stu}$ et $(\frac{a}{s}.\frac{b}{t})+(\frac{a}{s}.\frac{c}{u})=\frac{absu+acst}{s^2tu}$. Il sont égaux car $1.\big((absu+acst)stu-(abu+act)s^2tu\big)=0$.

— L'élément unitté est $\frac{1}{1}$.

— Le produit est commutatif $\frac{a}{s}.\frac{b}{t}=\frac{b}{t}.\frac{a}{s}$.

3. Supposons que $0\in S$. Alors, pour tout $a,a'\in A$ et tout $s,s'\in S$, $\frac{a}{s}=\frac{a'}{s'}$ car $0(as'-a's)=0$. L'anneau S^{-1} est donc trivial.
4. Soit $f:a\in A\mapsto\frac{a}{1}\in S^{-1}A$, c'est un morphisme d'anneaux :

   — $f(ab)=\frac{ab}{1}=\frac{a}{1}.\frac{b}{1}=f(a)f(b)$,

   — $(f(a+b)=\frac{a+b}{1}=\frac{a.1+b.1}{1}=f(a)+f(b)$,

   — $f(1)=\frac{1}{1}$.

   Supposons que S ne contient pas de diviseurs de zéro. Soit $a\in\mathrm{Ker}(f)$. Alors $f(a)=\frac{a}{1}=\frac{0}{1}$, donc il existe $u\in S$ tel que $u(a.1-1.0)=au=0$. Comme S ne contient pas de diviseur de zéro, ceci implique que $a=0$. Donc $\mathrm{Ker}(f)=\{0\}$ et f est bien injectif.
5. Supposons A est intègre. On donc que $S=A\backslash\{0\}$ et une partie multiplicative de A. Soit $\frac{a}{s}$ un élément non nul de S^{-1} ; on doit montrer qu'il est inversible. Comme $S=A\backslash\{0\}$ et $a\neq 0$, on a que $a\in S$ donc $\frac{s}{a}$ est un élément de $S^{-1}A$; il vérifie $\frac{a}{s}.\frac{s}{a}=\frac{1}{1}$ car $1.(as-sa)=0$.
6. Si P est un idéal premier de A, alors pour tout $s,t\in A\backslash P$, $st\in A\backslash P$ et $1\in A\backslash P$, donc $S=A\backslash P$ est bien multiplicative.
7. Pour montrer que l'idéal engendré par l'image de P dans A_P est le seul idéal maximal de A_P, démontrons d'abord qu'un élément $\frac{a}{s}$ est inversible dans A_P si et seulement si $a\notin P$. En effet, si $a\notin P$ alors $a\in S$ par définition de S et donc, comme $\frac{a}{s}.\frac{s}{a}=\frac{1}{1}$, $\frac{a}{s}$ est inversible dans A_P.
   Réciproquement, si $\frac{b}{t}$ est l'inverse de $\frac{a}{s}$ dans A_P alors il existe $u\in A\backslash P$ tel quel $u(ab-st)=0$. Ceci est équivalent à dire qu'il existe $u\in A\backslash P$ tel que $uab=ust$, comme $ust\in A\backslash P$, on a que $uab\notin P$ et donc $a\notin P$ car P est un idéal.
   Soit maintenant I un idéal propre de A_P et soit $\frac{a}{s}\in I$. Comme $I\neq A_P$, on sait que $\frac{a}{s}$ n'est pas inversible et donc $a\in P$ de sorte que $\frac{a}{s}$ appartient à l'idéal engendré par l'image de P ($f(P)$ d'après les notation de 4.) dans A_P. On a donc montré que $I\subset A_P$ et l'idéal engendré par $f(P)$ est bien l'unique idéal maximal de A_P.

EXERCICE 3. Montrer qu'un anneau A est un corps si et seulement si l'ensemble de ses idéaux a exactement deux éléments.

SOLUTION. Supposons que A est un corps. Soit I un idéal de A. Si $I\neq\{0\}$ alors il existe $x\in I$, $x\neq 0$. Comme A est un corps, x est inversible ie $\exists x^{-1}$ tel que $xx^{-1}=1\in I$ car I est un idéal. Donc $I=A$.
Réciproquement, supposons que A a exactement deux idéaux et montrons que tout élément non nul de A est inversible. Soit $a\in A$, $a\neq 0$. L'idéal engendré par a dans A, est alors , soit égal à $\{0\}$, ce qui n'est pas possible car dans ce cas $a=0$, soit il est égal à A, en particulier, il existe $a'\in A$ tel que $aa'=1$.

EXERCICE 4. Soit A un anneau factoriel. On suppose qu'il vérifie le théorème de Bezout, i.e. pour tous $a,b\in A$ premiers entre eux, il existe $u,v\in A$ avec $ua+vb=1$.

1. Montrer que si $a,b\in A$ ont pour pgcd d, alors il existe $u,v\in A$ avec $ua+bv=d$.
2. Montrer que si une famille finie $a_1,...,a_n$ d'éléments de A a pour pgcd 1, alors il existe des éléments $u_1,...,u_n$ de A avec $\sum_{i=1}^{n}u_ia_i=1$.
3. Montrer que si I est un idéal de A, alors il existe une famille finie d'éléments de I dont le pgcd est le pgcd de tous les éléments de I.
4. En déduire que A est principal.

SOLUTION.

1. Immédiat en notant que a/d et b/d sont premiers entre eux (noter que comme A est intègre et a,b sont divisibles par d, a/d et b/d ont bien un sens).

2. Par récurrence sur n. C'est clair pour $n \leq 2$ avec l'hypothèse. Supposons le résultat vrai jusqu'à $n-1$. Soit $d = \text{pgcd}(a_1, ..., a_{n-1})$. Alors il existe u, v dans A avec $ud + va_n = 1$ car $\text{pgcd}(d, a_n) = 1$ par définition du pgcd. Ensuite, l'hypothèse de récurrence appliquée à $a_1/d, ..., a_{n-1}/d$ donne une décomposition

$$d = u_1 a_1 + ... + u_{n-1} a_{n-1}, \quad u_1, ..., u_{n-1} \in A,$$

d'où on déduit le résultat.

3. Si I est nul ou $I = A$, c'est clair (si $I = A$ le pgcd de tous ses éléments est évidement 1). Sinon I contient un élément non nul et non inversible a, qu'on peut écrire

$$a = u. \prod_{i=1}^{r} p_i^{v_i(a)},$$

avec $u \in A^*$, $v_i(a) \in \mathbb{N}$, et les p_i irréductibles non associés deux à deux. Soit alors, pour chaque i, a_i un élément de I tel que $w_i := v_i(a_i)$ soit minimum parmi les $v_i(x)$ avec $x \in I$. Le pgcd de tous les éléments de I est alors

$$\prod_{i=1}^{r} p_i^{w_i},$$

qui est aussi le pgcd de $a_1, ..., a_r$.

4. Soient I un idéal de A et d le pgcd de tous les éléments de I. D'après c), c'est aussi le pgcd d'une famille finie $a_1, ..., a_r$ d'éléments de I. En appliquant b) à $a_1/d, ..., a_r/d$, on obtient que $d \in I$, d'où $(d) \subset I$. Par ailleurs $I \subset (d)$ par définition du pgcd de tous les éléments de I. Finalement I est bien principal.

EXERCICE 5. Soit A un anneau intègre. On dit que deux idéaux I et J de A sont *étrangers* si $I + J = A$ (de manière équivalente, cela signifie que 1 appartient à l'idéal $I + J$).

1. Montrer que si I_1 et I_2 sont tous deux étrangers avec J, alors l'idéal $I_1 I_2$ (constitué des sommes d'éléments de la forme $a_1 a_2$ avec $a_1 \in I_1$ et $a_2 \in I_2$) est encore étranger avec J.
2. On suppose que A est factoriel et que tout idéal premier non nul de A est maximal. Montrer que si $p \in A$ est irréductible et ne divise pas a, alors (p) est étranger avec (a).
3. On garde les hypothèses de b). Montrer que si $a, b \in A$ sont premiers entre eux, les idéaux (a) et (b) sont étrangers. En déduire que A est principal en utilisant l'exercice 4 de cette feuille.

SOLUTION.

1. Par hypothèse on peut écrire $1 = a_1 + b = a_2 + c$ avec $a_1 \in I_1$, $a_2 \in I_2$, et $b, c \in J$. En faisant le produit, on obtient $1 = a_1 a_2 + (a_1 c + b a_2 + bc)$ avec $a_1 a_2 \in I_1 I_2$ et $(c + b a_2 + bc) \in J$, ce qui montre que $I_1 I_2$ est encore étranger avec J.
2. L'idéal (p) est premier non nul car A est factoriel et p irréductible, il est donc maximal. Comme p ne divise pas a, l'idéal (a, p) contient strictement (p), il est donc égal à A, ce qui montre que (p) est étranger avec (a).
3. Écrivons la décomposition de a :

$$a = u p_1 ... p_r,$$

avec $u \in A^*$ et les p_i irréductibles. Comme a et b sont premiers entre eux, p_i ne divise pas b, et d'après b), (p_i) est étranger avec (b). D'après a) et par une récurrence facile, $(p_1)...(p_r) = (a)$ est étranger avec b. On peut donc écrire $a = va + wb$ avec v, w dans A. L'exercice 2 de cette feuille montre alors que A est principal, car il est factoriel et vérifie le théorème de Bezout. Noter que A n'avait pas été supposé noethérien au départ (il existe des anneaux intègres non noethériens tels que tout idéal premier non nul soit maximal, par exemple la fermeture intégrale de l'anneau $\mathbb{Z}_p$ des entiers p-adique dans la clôture algébrique $\overline{\mathbb{Q}_p}$ de son corps des fractions $\mathbb{Q}_p$).

EXERCICE 6. Dans l'anneau $A = \mathbb{Z}[i\sqrt{5}]$, trouver deux éléments qui n'ont pas de pgcd.

SOLUTION. Via les deux décompositions différentes en irréductibles

$$9 = 3.3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

on voit facilement que 9 et $3(2 + i\sqrt{5})$ n'ont pas de pgcd dans A.

EXERCICE 7. Soit H l'anneau des fonctions holomorphes de $\mathbb{C}$ dans $\mathbb{C}$.

1. Montrer que H est intègre. Quel est son corps des fractions ?
2. Montrer que H^* est constitué des fonctions qui ne s'annulent pas, et que l'ensemble des irréductibles de H est constitué des fonctions qui ont un seul zéro avec de plus ce zéro simple.
3. Montrer que H n'est ni factoriel ni noethérien, en exhibant un élément non inversible qui ne se décompose pas en produit d'irréductibles.

SOLUTION.

1. Les zéros d'une fonction holomorphe non nulle sont isolés. On en déduit immédiatement que le produit de deux fonctions holomorphes non nulles est non nulle, et donc que l'anneau non nul H est intègre. Son corps des fractions est par définition le corps des fonctions méromorphes sur $\mathbb{C}$.
2. Si f est holomorphe et ne s'annule pas, on sait que $1/f$ est holomorphe et donc $f \in H^*$. En sens inverse s'il existe g tel que $fg = 1$, il est clair que f ne s'annule pas.

   Si maintenant f est irréductible, elle n'est pas inversible, donc possède un zéro a. On sait alors que la fonction g définie par $g(z) = f(z)/(z-a)$ est encore dans H, et comme $h : z \mapsto (z-a)$ n'est pas inversible, la fonction g doit être inversible ce qui montre que a est le seul zéro de f et qu'il est simple. En sens inverse, si f admet a comme unique zéro et ce zéro est simple, alors si $f = f_1 f_2$ avec f_1, f_2 dans H, l'une des fonctions f_1, f_2 ne s'annule pas donc est dans H^*, ce qui montre que f est irréductible. On a en fait montré qu'un système de représentants irréductibles est constitué des fonctions de la forme $z \mapsto (z-a)$ avec $a \in \mathbb{C}$.
3. Soit une fonction holomorphe non nulle possédant une infinité de zéros, par exemple $z \mapsto \sin z$. Alors d'après 2., elle ne peut pas s'écrire comme produit d'un inversible et d'un nombre fini d'irréductibles, donc H n'est ni factoriel ni noethérien. On peut par contre montrer (plus difficile) que H vérifie le théorème de Bezout, ou encore que tout idéal *de type fini* de H est principal.

EXERCICE 8. Pour un anneau commutatif A et un idéal I de A, on définit le *radical de* I comme étant l'ensemble

$$\sqrt{I} = \{x \in A \mid \exists n \geq 1 \text{ tel que } x^n \in I\}.$$

1. Montrer que $\sqrt{I}$ est un idéal de A et que $\sqrt{\sqrt{I}} = \sqrt{I}$.
2. Montrer que si P est un idéal premier de A, alors $\sqrt{P} = P$.
3. Soit $x \notin \sqrt{I}$ et soit $S = \{x^n \mid n \in \mathbb{N}\}$. Montrer que S est une partie multiplicative de A qui est disjointe de I. En considérant l'anneau $S^{-1}A$, en déduire qu'il existe un idéal premier P contenant I mais pas x.
4. En déduire que $\sqrt{I}$ est l'intersection de tous les idéaux premiers de A contenant I (on suppose ici que I est différent de A).
5. Le *nilradical* de A est l'ensemble de tous les éléments *nilpotents* de A :

   $$\mathcal{N}(A) = \{x \in A \mid \exists n \in \mathbb{N} \text{ tel que } x^n = 0\}.$$

   Montrer que le nilradical de A est un idéal, et que c'est l'intersection de tous les idéaux premiers de A.

SOLUTION.

1. $I \subset \sqrt{I}$ donc $I \neq \emptyset$. Si $x, y \in \sqrt{I}$, il existe $n, m \geq 1$ tels que $x^n \in I$, $y^m \in I$. En utilisant le fait que I est un idéal, on a que $(x+y)^{n+m} = x^n x^m + x^n x^{m-1} y + x^n x^{m-2} y^2 + \ldots + x^n y^m + x^{n-1} y^m y + \ldots + x y^{n+m-1} + y^n y^m \in I$. Il est évident que $0 \in \sqrt{I}$ et que $-x \in \sqrt{I}$. Par ailleurs, comme A est commutatif, on que si $a \in A$ alors $(x.a)^n = x^n a^n \in I$. Comme $I \subset \sqrt{I}$, on a $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Si $x \in \sqrt{I} \subset \sqrt{\sqrt{I}}$, il existe $n \geq 1$ tel que $x^n \in \sqrt{I}$ donc il existe $m \geq 1$ tel que $(x^n)^m = x^{nm} \in I$ de sorte que $x \in \sqrt{I}$. Donc $I = \sqrt{\sqrt{I}}$.
2. Soit $x \in \sqrt{P}$ et $n \geq 1$ tel que $x^n = x.x^{n-1} \in P$. Comme P est premier on a que soit $x \in P$ et on arrête soit $x^{n-1} \in P$; dans ce dernier cas on a que $x^{n-1} = x x^{n-2} \in P$, donc soit $x \in P$ soit $x^{n-2} = x x^{n-3} \in P$; on continue ainsi jusqu'à obtenir $x \in P$. On a donc $\sqrt{P} = P$.

3. Soit $x \notin \sqrt{I}$ et $S = \{x^n \mid n \in \mathbb{N}\}$. S est multiplicative : $x^n, x^m \in S$ alors $x^n x^m = x^{n+m} \in S$ et $1 = x^0 \in S$. Supposons $y \in S \cap I$. Alors $y = x^n \in I$ donc $x\sqrt{I}$ ce qui est faux par hypothèse. On a donc bien que $S \cap I = \emptyset$.
Soit $\phi : A \to S^{-1}A$ le morphisme qui a $a \in A$ l'envoie vers la classe $\frac{a}{1} \in S^{-1}A$. Notons J l'idéal de $S^{-1}A$ engendré par $\phi(I)$. Soit M un idéal maximal de $S^{-1}A$ qui contient J. Alors, $P = \phi^{-1}(M)$ est un idéal premier de A disjoint de S. En effet, P est premier car M est premier et ϕ est un morphisme d'anneaux (facile à vérifier) et supposons $a \in P \cap S$ de sorte que $\phi(a) = \frac{a}{1} \in I$ Comme $a \in S$, $\frac{1}{a}$ existe et $\frac{a}{1}$ est inversible ce qui impliquerait que $M = S^{-1}A$. On a donc $P \cap S = \emptyset$. On a que $x \notin P$ car $x \in S$ et donc $\frac{x}{1} \notin M$ car il est inversible dans $S^{-1}A$. Et $I \subset P$ car $phi(I) \subset M$ et $\phi(I) \neq S^{-1}A$ car $x \neq \sqrt{I}$.
4. Si x appartient à l'intersection de tous les idéaux premiers de A qui contiennent I alors $x \in \sqrt{I}$ car sinon, on vient de montrer qu'il existe un idéal premier de A qui contient I et qui ne contient pas x. Montrons maintenant que $\sqrt{I}$ est inclus dans l'intersection de tous les idéaux premiers de A qui contiennent I : si $x \in \sqrt{I}$, alors $\exists n \geq 1$ tel que $x^n \in I$. Soit P un idéal premier de A qui contient I. Dans ce cas $x^n = xx^{n-1} \in P$, donc soit $x \in P$ soit $x^{n-1} \in P$ Par récurrence, on obtient que $x \in P$; donc $\sqrt{I} \subset P$. Et on a montré que $\sqrt{I}$ est égal à l'intersection de tous les idéaux premiers de A qui contiennent I.
5. Il est facile de montrer que $\mathcal{N}(A)$ est un idéal de A. Par défintion $\mathcal{N}(A) = \sqrt{\{0\}}$ donc par la question précédente on a bien que $\mathcal{N}(A)$ est l'intersection de tous les idéaux premiers de A.

EXERCICE 9. Soit $\mathbb{Z}[i]$ l'anneau des entiers de Gauss.

1. Soit p un nombre premier. Montrer que p est irréductible dans $\mathbb{Z}[i]$ si, et seulement si, p ne s'écrit pas comme somme de deux carrés d'entiers.
2. Soit p un nombre premier congru à 3 modulo 4. Montrer que si pour deux entiers a et b, on a $a^2 + b^2 \equiv 0 \bmod p$, alors p divise a et b.
3. Montrer qu'une somme de deux carrés d'entiers est congrue à 0, 1 ou 2 modulo 4.
4. En déduire qu'un nombre premier p est irréductible dans $\mathbb{Z}[i]$ si, et seulement si, $p \equiv 3 \bmod 4$. (Indication : on pourra calculer $(p-1)! \bmod p$).

SOLUTION. $\mathbb{Z}[i]$ est un anneau euclidien de stathme $N : a + bi \in \mathbb{Z}[i] \mapsto a^2 + b^2\mathbb{N}$. Il est facile de voir que N est multiplicative ie si $z, z' \in \mathbb{Z}[i]$ alors $N(zz') = N(z)N(z')$. On a aussi que $z \in \mathbb{Z}[i]$ est inversible si et seulement si $N(z) = 1$.

1. Montrons le sens direct par contraposée. Supposons qu'il existe $a, b \in \mathbb{Z}$ tel que $p = a^2 + b^2$. Alors $p = (a+ib)(a-ib)$ n'est pas irréductible.
Réciproquement, supposons $p = uv$ avec $u, v \notin \mathbb{Z}[i]^*$, alors $N(p) = N(u)N(v) = p^2$; donc $N(u)$ divise p^2 et comme u n'est pas inversible, $N(u) \neq 1$ et donc $N(u) = p$ (si $N(u) = p^2$ on aurait que $N(v) = 1$ mais v n'est pas inversible non plus. Donc $p = N(u) = u_1^2 + u_2^2$ où $u = u_1 + iu_2 \in \mathbb{Z}[i]$; c'est la somme de deux carrés.
2. Soit $p \equiv 3[4]$. Soient $a, b \in \mathbb{Z}$ tels que $a^2 + b^2 \equiv 0[p]$. Supposons $b \not\equiv 0[p]$ alors b est inversible dans $(\mathbb{Z}/p\mathbb{Z})$ et $(ab^{-1})^2 \equiv a^2(b^{-1})^2 \equiv -b^2(b^2)^{-1} \equiv -1[p]$; on a aussi que $a^2 \not\equiv 0[p]$ car $b^2 \not\equiv 0[p]$ et $a^2 \equiv -b^2[p]$. Si on pose $x = ab^{-1}$ on a alors que $x \not\equiv 0[p]$ et $x^2 \equiv -1[p]$; autrement dit -1 est un carré modulo p. Mais $(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1$ car l'ordre de $(\mathbb{Z}/p\mathbb{Z})^\times$ est $p-1$. Donc, $\frac{p-1}{2}$ doit être pair et $p \equiv 1[4]$ ce qui est une contradiction car on supposé $p \equiv 3[4]$. On a donc montré que $b \equiv 0[p]$. De même, si on suppose $a \not\equiv 0[p]$ on arrive à une contradiction et $a \equiv 0[p]$ aussi.

3. Pour tout entier $a \in \mathbb{Z}$ les classes possibles modulo 4 de a^2 sont : 0 ou 1 ; donc pour $a, b \in \mathbb{Z}$ les possibles classes pour $a^2 + b^2$ modulo 4 sont 0, 1 ou 2.
4. Montre que les trois conditions suivantes sont équivalentes
   (a) p est irréductible,
   (b) $p \equiv 3[4]$,
   (c) p n'est pas la somme de deux carrés.

   C'est facile de voir que (b) implique (c) : d'après la question 3. si $p = a^2 + b^2$ alors $p \not\equiv 3[4]$. Montrons que (a) implique (b). Supposons p irréductible dans $\mathbb{Z}[i]$. Si $p \equiv 1[4]$ alors on montre à l'aide du Théorème de Wilson qu'il

existe $x \in \mathbb{Z}$ tel que $x^2 \equiv -1[p]$. Dans ce cas p divise $x^2+1 = (x+i)(x-i)$ or on a supposé que p était irréductible donc on a forcément que p divise $(x+i)$ ou $(x-i)$. En effet, p s'écrit comme $p = 2k+1$ avec k un entier pair et on écrit $(p-1)! = 2k(2k-1)\dots(k+1)k(k-1)\dots 2.1$. Comme pour tout $i \in \{0,\dots,k-1\}$ on a que $2k-i \equiv -(i+1)[p]$, on a que

$$\begin{aligned}(p-1)! &= -1 \times -2^2 \times \dots (-(i+1)^2) \times \dots \times (-(k-1)^2) \times (-k^2)\\ &= (-1)^k \times 2^2 \times 3^2 \times \dots \times (k-1)^2 \times k^2\\ &= (-1)^k (k!)^2\\ &\equiv -1[p]\end{aligned}$$

d'après le Théorème de Wilson. Comme k est pair on a alors que $(k!)^2 \equiv -1[p]$ et donc -1 est bien un carré modulo p.

EXERCICE 10. Soit A le sous-anneau de $\mathbb{C}$ engendré par $\alpha = \frac{1+i\sqrt{19}}{2}$. Le but de cet exercice est de montrer que A est principal, mais pas euclidien.

1. Montrer d'abord que, si B est un anneau euclidien, alors il existe un élément non inversible $x \in B$ tel que la restriction à $B^* \cup \{0\}$ de la projection de B sur $B/(x)$ soit surjective. Ceci nous servira de critère pour montrer que l'anneau A n'est pas euclidien.
2. Donner un polynôme du second degré à coefficients entiers P s'annulant en α. En déduire que A est isomorphe à $\mathbb{Z}[X]/P$ et que le groupe abélien sous-jacent à A est engendré par 1 et α. Vérifier que l'application norme, qui à $z \in A$ associe $N(z) = z\overline{z}$, prend ses valeurs dans $\mathbb{N}$.
3. Montrer que 1 et -1 sont les seuls éléments inversibles de A.
4. Montrer qu'il n'existe pas de morphisme surjectif d'anneaux de A dans $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$ (indication : pour chacun des deux cas, supposer que f soit une telle surjection, et étudier l'image par f du polynôme trouvé en (2)).
5. En déduire que A n'est pas euclidien (indication : utiliser le critère de (1)).
6. On va montrer que A est principal.
   (a) Montrer que pour tout a, b éléments non nuls de A, il existe $q, r \in A$ tels que $r = 0$ ou $N(r) < N(b)$ et qui vérifient, soit $a = bq + r$, soit $2a = bq + r$.
   (b) Montrer que l'idéal engendré par 2 est maximal dans A (on pourra utiliser le fait que A est isomorphe à un quotient de $\mathbb{Z}[x]$).
   (c) Montrer que A est principal.

SOLUTION.

1. Supposons B euclidien et notons v son stathme. On doit montrer qu'il existe $x \in B$ non inversible tel que, si on note (x) l'idéal de B engendré par x, pour tout $a \in B$ il existe $b \in B^* \cup \{0\}$ tel que $b + (x) = a + (x)$ ie tel que $a = qx + b$ pour $q \in B$ et b inversible.
   Si B est un corps il suffit de prendre $x = 0$. Sinon, soit $x \in B\backslash(B^* \cup \{0\})$ tel que $v(x)$ soit minimal dans $B\backslash(B^* \cup \{0\})$. Comme B est euclidien, pour tout $a \in B$ il existe $q, b \in B$ tels que $a = qx + b$ avec $b = 0$ ou $v(b) < v(x)$. Si $b = 0$ on a que $a \in (x)$ et donc $p(0) = p(a)$. Sinon, $v(b) < v(x)$ implique que b est inversible et $p(b) = p(a)$.
2. $\alpha = \frac{1+i\sqrt{9}}{2}$ est racine de $P(X) = X^2 - X + 5$ car $(X-\alpha)(X-\overline{\alpha}) = X^2 - (\alpha+\overline{\alpha})X + \alpha\overline{\alpha}$. Montrons que A est isomorphe à $\mathbb{Z}[X]/P$. Pour tout $F \in \mathbb{Z}[X]$ il existe Q, R tels que $F = QP + R$ où $R = 0$ ou $\deg(R) < \deg P = 2$ car le coefficient dominant de P est inversible dans $\mathbb{Z}$. On peut donc définir un morphisme π de $\mathbb{Z}[X]$ dans $\mathbb{Z}[X]/(P)$ qui a F associe R, le reste de la division euclidienne de F par P. Comme $P(\alpha) = 0$ le morphisme

$$\begin{aligned}\varphi : \mathbb{Z}[X] &\to \mathbb{Z}[\alpha]\\ X &\mapsto \alpha\end{aligned}$$

   se factorise par (P) et on obtient un morphisme $\tilde{\varphi} : \mathbb{Z}[X]/(P) \to \mathbb{Z}[\alpha]$ tel que $\varphi = \tilde{\varphi} \circ \pi$. $\tilde{\varphi}$ est en fait surjectif : comme $\alpha^2 = \alpha - 5$ on sait que 1 et α engendrent $\mathbb{Z}[\alpha]$. Si $R(X) \in \mathbb{Z}[X]/(P)$ alors R est de la forme $R(X) = aX + b$ car $\deg(R) < 2$ et donc $\tilde{\varphi}(aX + b) = a\alpha + b$. On a en plus que $\tilde{\varphi}$ est injectif : si $\tilde{\varphi}(aX + b) = \tilde{\varphi}(a'X + b')$ alors

$alpha$ est racine de $(a-a')X+b-b'=0$ donc $\alpha=\frac{b'-b}{a-a'}\in\mathbb{Q}$; or $\alpha=\frac{1+i\sqrt{19}}{2}$ donc $a=a'$ et $b=b'$. On en déduit que $\mathbb{Z}[X]/(P)\simeq\mathbb{Z}[\alpha]$.
On vérifie facilement que pour $z=a\alpha+b\in\mathbb{Z}[\alpha]$, $N(z)=z\overline{z}=(a\alpha+b)(\overline{a\alpha+b})=5a^2+ab+b^2\in\mathbb{N}$.

3. Supposons z inversible et z' tel que $zz'=1$. Alors $N(zz')=N(z)N(z')=1$, donc $N(z)=1$. Si $z=a\alpha+b$ on a que $5a^2+ab+b^2=1$ donc $a=0$ et $b=\pm1$ donc $z=\pm1$. On vérifie ensuite que 1 et -1 sont effectivement inversibles et donc $\mathbb{Z}[\alpha]^*=\{-1,1\}$.

4. Supposons $f:A\to\mathbb{Z}/2\mathbb{Z}$ morphisme. Comme $\alpha^2-\alpha+5=0$ dans A, on a que $b^2-b+5=b^2-b+1=0$ dans $\mathbb{Z}/2\mathbb{Z}$ où $b=f(a)$. Or, le polynôme X^2-X+1 n'a pas de racine dans $\mathbb{Z}/2\mathbb{Z}$; don cil n'y a pas de morphisme de A dans $\mathbb{Z}/2\mathbb{Z}$. De même si $f:A\to\mathbb{Z}/3\mathbb{Z}$ on aurait $\beta\in\mathbb{Z}/3\mathbb{Z}$ tel que $\beta^2-\beta-1$ mais X^2-X-1 n'a pas de racines dans $\mathbb{Z}/3\mathbb{Z}$.

5. Supposons A euclidien ; d'après 1. il existe x non inversible tel que la restriction de $p:A\to A/(x)$ à $A^*\cup\{0\}$ est surjective. Comme $A\simeq\mathbb{Z}[\alpha]$, on a $A^*:\{-1,1\}$ et $p|_{A^*\cup\{0\}}:\{-1,1,0\}\to A/(x)$ est surjective. On montre que $A/(x)$ est un corps : pour tout $a+(x)\in A/(x)$ il existe b inversible ou $b=0$ tel que $a+(x)=b+(x)$. Si $b=0$ alors $a\in(x)$ est l'élément neutre de $A/(x)$; si b est inversible alors $p(b)=a+(x)$ est inversible. $A/(x)$ est donc un corps. Comme $p|_{A^*\cup\{0\}}$ est surjective le cardinal de $A/(x)$ est inférieur ou égal à 3, $A/(x)$ est donc isomorphe soit à $\mathbb{Z}/2\mathbb{Z}$ soit à $\mathbb{Z}/3\mathbb{Z}$. On aurait donc un morphisme surjectif de A dans $\mathbb{Z}/2\mathbb{Z}$ ou dans $\mathbb{Z}/3\mathbb{Z}$, ce qui est impossible. Donc A n'est pas euclidien.

6. (a) Soient $a,b\in A$ non nuls. Soit $x=\frac{a}{b}\in\mathbb{C}$; il s'écrit $x=u+v\alpha$ avec $u,v\in\mathbb{Q}$. ($x=\frac{a\overline{b}}{b\overline{b}}=\frac{1}{N(b)}(a\overline{b})\in\mathbb{Q}[\alpha]$).
Soit n la partie entière de v. Alors $v\in[n,n+1[$. Supposons $v\notin]n+\frac{1}{3},n+\frac{2}{3}[$ et soient s,t les entiers les plus proches de u et de v respectivement. Alors $|s-u|\leq\frac{1}{2}$, $|t-v|\leq\frac{1}{3}$. On pose $q=s+t\alpha$ et donc $q\in A=\mathbb{Z}[\alpha]$. On a alors que $N(x-q)=N((u-s)+(v-t)\alpha)=(s-u)^2+(s-u)(t-v)+5(t-v)^2\leq\frac{1}{4}+\frac{1}{6}+\frac{5}{9}<1$. On pose $r=a-bq$. On a alors que $a=bq+r$ et $N(r)<N(b)$.
Supposons maintenant $v\in]n+\frac{1}{3},n+\frac{2}{3}[$. On prend $2x=2u+2v\alpha$ et $2v\in]2n+\frac{2}{3},2n+1+\frac{1}{3}[$, si m est la partie entière de $2v$ alors $2v\notin]m+\frac{1}{3},m+\frac{2}{3}[$. On se ramène donc au cas précédent et $2a=bq+r$ avec $N(r)<N(b)$.

   (b) Montrer que l'idéal engendré par 2 est maximal dans A (on pourra utiliser le fait que A est isomorphe à un quotient de $\mathbb{Z}[x]$). On a que $A\simeq\mathbb{Z}[X]/(X^2-X+5)$ donc

$$A/(2)\simeq\mathbb{Z}[X]/(2,X^2-X+5)\simeq(\mathbb{Z}/2\mathbb{Z})[X]/(X^2-X+5)\simeq(\mathbb{Z}/2\mathbb{Z})[X]/(X^2+X+1)$$

   et X^2+X+1 comme est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$, on a que $A/(2)$ est un corps.

   (c) Soit I un idéal non nul de A et $a\in I$, $a\neq0$ tel que $N(a)$ soit minimal. Si $I=(a)$ il est principal. Sinon, alors soit $x\in I\backslash(a)$. Si $x=aq+r$ avec $N(r)<N(a)$ ou $r=0$, comme $x,a\in I$ on a que $r\in I$ et donc $r=0$ car $N(a)$ est minimal dans I. Dans ce cas $x\in(a)$, contradiction.
Si $2x=aq+r$, $N(r)<N(a)$ ou $r=0$, on a aussi $r=0$ et $2x=aq$ donc $aq\in(2)$. Comme (2) est maximal, il est premier donc soit $a\in(2)$ soit $q\in(2)$. Si $q\in(2)$, alors q est de la forme $q=2q'$, donc $2x=a2q'$ donc $2(x-aq)=0$ ce qui implique que $x=qa$ car A est intègre. Donc $x\in(a)$ contradiction. On a donc que $a\in(2)$. Donc a est de la forme $a=2a'$ et $x=a'q\in(a')$; comme $N(a)=N(2)N(a')$ on a $N(a')<N(a)$. Montrons que $a'\in I$. Comme (2) est maximal et $q\notin(2)$ on a que l'idéal engendré par 2 et q, $(2,q)$ est égal à A. ; il existe alors $\lambda,\mu\in A$ tels que $2\lambda+q\mu=1$, ce qui implique que $a'=2\lambda a'+q\mu a'=a\lambda+\mu x\in I$. Mais $N(a)$ est minimal dans I, donc on arrive à une contradiction. On a bien que $I=(a)$ et A est principal.

EXERCICE 11. Le *radical de Jacobson* d'un anneau commutatif A est l'intersection de tous les idéaux maximaux de A. On le note rad A.

1. Soit A un anneau. Montrer qu'un élément a est dans le radical de Jacobson de A si, et seulement si, pour tout $x\in A$, $1-ax$ est inversible.
2. Montrer que si $x\in A$ est nilpotent, alors $1-ax$ est inversible, $\forall a\in A$.
3. Montrer que le radical de Jacobson de A est le plus grand idéal de A tel que $1-x$ est inversible pour tout $x\in\text{rad}\,A$.
4. Soit I un idéal dont tous les éléments sont nilpotents. Montrer que $I\subseteq\text{rad}\,A$.
5. Calculer le radical de Jacobson de $\mathbb{Z}$, $\mathbb{R}[X]$, $\mathbb{Z}/n\mathbb{Z}$ (pour un entier $n>1$).

SOLUTION. 1. Soit $a \in \mathrm{rad}(A)$. Alors $a \in M$ pour tout idéal maximal de A et l'idéal engendré par a, vérifie $(a) \subset M$ pour tout idéal maximal M de A. Soit $x \in A$ et supposons $1 - ax$ non inversible ; alors il existe un idéal maximal M tel que $(1 - ax) \subset M$, donc en particulier il existe $m \in M$ tel que $1 = ax + m$ et donc $1 \in M$ car $ax \in M$ si $(a) \subset M$, ce qui implique que $M = A$, contradiction. On a donc bien que $1 - ax \in A^*$.
Réciproquement, supposons $1 - ax \in A^*$ pour tout $x \in A$. Montrons que $a \in \mathrm{rad}(A)$. Supposons que ce n'est pas le cas ; il existe donc un idéal maximal M de A tel que $a \notin M$. Dans ce cas l'idéal engendré par M et a (ie le plus petit idéal qui contient a et M) est égal à A. Il existe donc $x \in A$ et $m \in M$ tels que $1 = m + ax$, d'où $m = 1 - ax$ qui ne peut pas être inversible car $m \in M \neq A$. On arrive donc a une contradiction et on a que, pour tout idéal maximal M de A, $a \in M$ et donc $a \in \mathrm{rad}(A)$.

2. Soit $x \in A$ nilpotent, c'est-à-dire qu'il existe un entier $n > 1$ tel que $x^n = 0$. On a donc que $1 = 1 - x^n = (1 - x)(1 + x + \cdots + x^{n-1})$ et donc $(1 - x)$ est inversible d'inverse $(1 + x + \cdots + x^{n-1})$. Mais si $x^n = 0$ on a aussi que, pour tout $a \in A$, $(ax)^n = a^n x^n = 0$ car A est supposé commutatif ; donc $1 = 1-(ax)^n = (1-ax)(1+ax+\cdots+(ax)^{n-1})$ et $1 - ax$ est inversible d'inverse $(1 + ax + \cdots + (ax)^{n-1})$.

3. On a montré que pour tout $x \in \mathrm{rad}(A)$, $1 - x \in A^*$. Soit I un idéal de A tel que, pour tout $x \in I$, $1 - x \in A^*$. Soit $x \in I$ et supposons $x \notin \mathrm{rad}(A)$. Il existe alors un idéal maximal K de A tel que $x \notin K$ et l'idéal engendré par x et K, (x, K) étant le plus petit idéal qui contient K et x, est égal à A. Cela implique qu'il existe $a \in A$ et $k \in K$ tels que $1 = xa + k$. Or $k = 1 - xa \in A^*$ (car comme $x \in I$, on a que $xa \in I$). L'idéal K contient alors un élément inversible et il est égal à A, ce qui est une contradiction car K est maximal. On a donc que $x \in \mathrm{rad}(A)$ et alors $I \subset \mathrm{rad}(A)$.

4. Soit I un idéal tel que tout élément de I est nilpotent ; alors tout élément x de I vérifie que $1 - x$ est inversible et $I \subset \mathrm{rad}(A)$.

5. Si $n \in \mathrm{rad}(\mathbb{Z})$ alors pour tout entier k, $1 - nk \in Z^* = \{-1, 1\}$, ce qui implique forcément que $\mathrm{rad}(\mathbb{Z}) = \{0\}$.
Si $P \in \mathrm{rad}(\mathbb{R}[X])$ alors $1 - PQ$ est inversible pour tout $Q \in \mathbb{R}[X]$; en particulier $1 - XP$ est inversible, ce qui implique $P = 0$; $\mathrm{rad}(\mathbb{R}[X]) = \{0\}$.
Les idéaux premiers de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $p\mathbb{Z}/n\mathbb{Z}$ où p est un nombre premier qui divise n. On a alors que $\mathrm{rad}(\mathbb{Z}/n\mathbb{Z}) = \bigcap_{i=1}^{k} p_i\mathbb{Z}/n\mathbb{Z} = (p_1, \ldots, p_k)\mathbb{Z}/n\mathbb{Z}$, où $p_1, \ldots, p_k$, $p_i \neq p_j$ sont les diviseurs premiers de n.

EXERCICE 12. Soit A un anneau euclidien de stathme φ [1]. Montrer que

1. il existe un stathme $\tilde{\varphi}$ qui vérifie la condition $\tilde{\varphi}(ab) \geq \tilde{\varphi}(a)$ pour tous $a, b \in A$ non nuls ;
2. pour tout $a \in A \setminus \{0\}$, $\tilde{\varphi}(a) \geq \tilde{\varphi}(1)$;
3. $\tilde{\varphi}(a) = \tilde{\varphi}(1)$ si, et seulement si, a est inversible dans A ;
4. si $a, b \in A \setminus \{0\}$ sont associés, alors $\tilde{\varphi}(a) = \tilde{\varphi}(b)$;
5. si $a, b \in A \setminus \{0\}$ sont tels que a divise b et $\tilde{\varphi}(a) = \tilde{\varphi}(b)$, alors a et b sont associés.

SOLUTION.

1. Il suffit de prendre $\tilde{\varphi}(a) = \min_{x \neq 0} \varphi(ax)$.
2. C'est évident.
3. Par division euclidienne : il existe $q, r \in A$ tels que $1 = aq + r$ avec $\tilde{\varphi}(r) < \tilde{\varphi}(a)$ ou $r = 0$; si $\tilde{\varphi}(a) = 1$ on a $r = 0$ et $a \in A^*$. Réciproquement, si $aa' = 1$, on a $\tilde{\varphi}(1) = \tilde{\varphi}(aa') \geq \tilde{\varphi}(a)$ et donc $\tilde{\varphi}(a) = \tilde{\varphi}(1)$.
4. Si $a = ub$ avec $u \in A^*$, $\tilde{\varphi}(a) = \tilde{\varphi}(ub) \geq \tilde{\varphi}(b)$ et $\tilde{\varphi}(b) = \tilde{\varphi}(u^{-1}a) \geq \tilde{\varphi}(a)$ donc $\tilde{\varphi}(a) = \tilde{\varphi}(b)$.
5. il existe $q \in A$ tel que $b = aq$ car a divise b. Aussi il existe $q', r \in A$ tels que $a = bq' + r$ avec $\tilde{\varphi}(r) < \tilde{\varphi}(b) = \tilde{\varphi}(a)$ ou $r = 0$; donc $a = aqq' + r$ et $\tilde{\varphi}(r) = \tilde{\varphi}(a(1 - qq')) \geq \tilde{\varphi}(a)$ et $r = 0$, donc b divise aussi a et ils sont donc associés.

1. en cours un stathme est défini comme étant un application $\varphi : A\setminus\{0\} \to \mathbb{N}$ telle que $\forall a \in A\ \forall b \in A\setminus\{0\}\ \exists q, r \in A$ tels que $a = bq + r$ avec $\varphi(r) < \varphi(b)$ ou $r = 0$. Dans d'autres références cette notion correspond à la notion de "préstathme" ; dans ce cas un stathme est un pré-stathme qui vérifie aussi la première condition à démontrer dans cet exercice