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[1] $\varphi_a : x \in A \mapsto ax$. Comme A est intègre on voit facilement que φ_a est injectif[2], 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 $f : A \longrightarrow S^{-1}A$ 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.
La localisation d'un anneau, qui consiste à rendre inversible une partie multiplicative et dont on verra l'origine de la terminologie dans l'exercice 13 (qui correspond à l'étude de comportement local de fonctions), est un outil indispensable en géométrie algébrique et théorie des nombres notamment.

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 $as - as = 0$ et $1 \in S$;
   - 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 $(a, s) \sim (c, k)$ car $uvt \in S$ car S est multiplicative.
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

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

   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 $\frac{a}{s}$, $\frac{b}{t}$, $\frac{c}{u} \in S^{-1}A$,

1. Attention à bien voir qu'il ne s'agit pas d'un morphisme d'anneaux si $a \neq 1$ car par exemple $\varphi_a(1) = a$.
2. En effet, si l'on se donne $x, x' \in A$ tels que $\varphi_a(x) = \varphi_a(x')$ soit $a(x - x') = 0$, comme $a \neq 0$ et A est intègre, on obtient bien $x - x' = 0$ soit $x = x'$. Comme on n'a pas un morphisme, il ne s'agit pas de regarder le noyau !

- $+$ 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 : $(\frac{a}{s}\cdot\frac{b}{t})\cdot\frac{c}{u}=\frac{abc}{stu}=\frac{a}{s}\cdot(\frac{b}{t}\cdot\frac{c}{u})$;
- La multiplication est distributive par rapport à l'addition : $\frac{a}{s}\cdot(\frac{b}{t}+\frac{c}{u})=\frac{abu+act}{stu}$ et $(\frac{a}{s}\cdot\frac{b}{t})+(\frac{a}{s}\cdot\frac{c}{u})=\frac{absu+acst}{s^2tu}$. Il sont égaux car $1\cdot\big((absu+acst)stu-(abu+act)s^2tu\big)=0$;
- L'élément unité est $\frac{1}{1}$;
- Le produit est commutatif $\frac{a}{s}\cdot\frac{b}{t}=\frac{b}{t}\cdot\frac{a}{s}$.

Noter que la présence du u dans la définition de la relation d'équivalence (qui peut paraître étrange à première vue dans l'optique de définir la fraction $\frac{a}{s}$) est en réalité essentielle pour obtenir la transitivité !

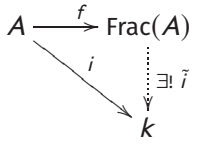
3. Supposons que $0\in S$. Alors, pour tout $a,a'\in A$ et tout $s,s'\in S$, $\frac{a}{s}=\frac{a'}{s'}$ car $0(as'-a's)=0$. L'anneau $S^{-1}A$ est donc trivial.

4. Soit $f:a\in A\mapsto\frac{a}{1}\in S^{-1}A$, c'est un morphisme d'anneaux :

- Pour tous $a,b\in A$, $f(ab)=\frac{ab}{1}=\frac{a}{1}\cdot\frac{b}{1}=f(a)f(b)$;
- Pour tous $a,b\in A$, $f(a+b)=\frac{a+b}{1}=\frac{a\cdot1+b\cdot1}{1}=f(a)+f(b)$;
- $f(1)=\frac{1}{1}$.

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 $S^{-1}A$; on doit montrer qu'il est inversible. Comme $S=A\backslash\{0\}$ et $a\neq0$, on a que $a\in S$ donc $\frac{s}{a}$ est un élément de $S^{-1}A$; il vérifie $\frac{a}{s}\cdot\frac{s}{a}=\frac{1}{1}$ car $1\cdot(as-sa)=0$. Le corps des fractions est le plus petit corps contenant A et il vérifie la propriété universelle suivante : si k est un corps et $i:A\to k$ est un morphisme injectif, alors il existe un unique morphisme de corps[3] $\tilde{i}:\mathrm{Frac}(A)\to k$ injectif tel que $\tilde{i}\circ f=i$, autrement dit tel que le diagramme suivant commute.



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 $\frac{a}{s}\cdot\frac{s}{a}=\frac{1}{1}$, $\frac{a}{s}$ 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.
Remarquons alors que $f(P)=\left\{\frac{p}{1}\ :\ p\in P\right\}$ n'est pas un idéal[4] de A_P. On considère donc $S^{-1}P$ l'idéal engendré par $f(P)$. Il est alors facile de voir que $\left\{\frac{p}{s}\ :\ p\in P,\ s\notin P\right\}$ est un idéal de A_P contenant $f(P)$ et que c'est le plus petit. Il s'agit donc de $S^{-1}P$.
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 $S^{-1}P$. On a donc montré que $I\subset S^{-1}P$ et l'idéal engendré par $f(P)$ est bien l'unique idéal maximal de A_P.
Noter qu'en composant la surjection canonique $\pi_P:A_P\to A_P/S^{-1}P$ avec le morphisme f de la question **4.**, il vient un morphisme de noyau P si bien qu'on obtient un morphisme injectif $A/P\to A_P/S^{-1}P$ défini par $\pi(a)\to\pi_P\left(\frac{a}{1}\right)$ avec

3. Je vous laisse vérifier que $\tilde{i}\left(\frac{a}{s}\right)=\frac{i(a)}{i(b)}$ est cet unique morphisme.

4. Par exemple car $\frac{p}{1}\cdot\frac{1}{s}=\frac{p}{s}\notin f(P)$ pour $s\in S\setminus\{1\}$.

$A_P/S^{-1}P$ un corps, appelé *corps résiduel*. Par propriété universelle du corps de fraction, on obtient un morphisme injectif $\mathrm{Frac}(A/P) \longrightarrow A_P/S^{-1}P$ donné par[5] $\frac{\pi(a)}{\pi(s)} \longrightarrow \pi_P\left(\frac{a}{s}\right)$ dont on peut montrer qu'il est surjectif. En effet, si $\pi_P\left(\frac{a}{s}\right)$ avec $s \notin P$, alors si l'on dénote par $\pi : A \longrightarrow A/P$ la surjection canonique, $\pi(s) \neq 0$ et alors $\frac{\pi(a)}{\pi(s)} \in \mathrm{Frac}(A/P)$ et est un antécédent de $\pi_P\left(\frac{a}{s}\right)$. On a donc $\mathrm{Frac}(A/P) \cong A_P/S^{-1}P$. Dans le cas de $A = \mathbf{Z}$ et $P = p\mathbf{Z}$ pour p premier, il vient que $\mathbf{Z}_{(p)}/S^{-1}p\mathbf{Z} \cong \mathbf{F}_p$. Noter qu'on a

$$\mathbf{Z}_{(p)} = \left\{\frac{a}{b} \ : \ p \nmid b\right\} = \mathbf{Z}\left[\frac{1}{\ell} \ : \ \ell \neq p \text{ premier}\right].$$

On appelle un tel anneau un anneau *local* sur lesquels on reviendra plus en détails dans l'exercice 13. On peut également montrer que le résultat ne se généralise pas à la partie multiplicative formée d'une réunion d'idéaux premiers. Dans ce cas, on obtient un anneau *sem-local* qui contient autant d'idéaux maximaux que d'idéaux premiers dans la réunion (exercice !).

On donne les exemples suivants dont les détails sont laissés e exercice :

- $\mathrm{Frac}(\mathbf{Z}) \cong \mathbf{Q}$;
- $\mathrm{Frac}(k[X]) \cong k(X)$ pour un corps k;
- Si $A = \mathbf{Z}$ et $S = \left\{10^k \ : \ k \in \mathbf{N}\right\}$, alors $S^{-1}A = \mathbf{D}$ l'ensemble des décimaux;
- Si $A = \mathbf{Z}$ et $S = \{\pm 1\}$, alors $S^{-1}A = \mathbf{N}$;
- $A = \mathbf{Z}^2$ et $S = \{(x, y) \ : \ (x, y) \in \mathbf{Z}^* \times \mathbf{Z}\}$, alors $S^{-1}A = \mathbf{Q} \times \mathbf{Z}$;
- Un idéal de $\mathbf{Z}/n\mathbf{Z}$ est par le théorème de correspondance la projection d'un idéal de $\mathbf{Z}$ contenant $n\mathbf{Z}$ donc par principalité de $\mathbf{Z}$, de la forme $d\mathbf{Z}$ avec $d \mid n$. L'image réciproque par un morphisme d'anneaux d'un idéal premier étant premier, on voit qu'un idéal premier de $\mathbf{Z}/n\mathbf{Z}$ provient d'un $p\mathbf{Z}$ avec $p \mid n$ premier et il n'est pas difficile de voir que le quotient de $\mathbf{Z}/n\mathbf{Z}$ par $p\mathbf{Z}/n\mathbf{Z}$ est isomorphe au corps $\mathbf{F}_p$ si bien qu'on a là tous les idéaux premiers de $\mathbf{Z}/n\mathbf{Z}$ qui sont également maximaux[6]. On vérifie alors que

$$(\mathbf{Z}/n\mathbf{Z})_{(p)} \cong \mathbf{Z}/p^\alpha\mathbf{Z}$$

pour $p \mid n$ premier et si $n = p^\alpha m$ avec $p \nmid m$. En effet, le morphisme[7] $\mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z} \longrightarrow (\mathbf{Z}/n\mathbf{Z})_{(p)}$ est surjectif. Soit $\frac{\pi(y)}{s} \in (\mathbf{Z}/n\mathbf{Z})_{(p)}$ avec $y \in \mathbf{Z}$ et $s \notin (p)$. Alors s et p^α sont premiers entre eux et il existe deux entiers u et v tels que $us + p^\alpha v = 1$. On a donc $m(suy - y) = mvyp^\alpha = nvy$ de sorte que $m(s\pi(uy) - \pi(y)) = 0$ dans $\mathbf{Z}/n\mathbf{Z}$ et $m \notin (p)$ si bien que $\frac{\pi(uy)}{1} = \frac{y}{s}$ et uy est un antécédent de $\frac{y}{s}$. On montre alors que le noyau de ce morphisme est $p^\alpha\mathbf{Z}$. Il est clairement contenu dans le noyau car $\frac{\pi(p^\alpha)}{1} = \frac{\pi(mp^\alpha)}{m} = 0$. Réciproquement, soit x dans le noyau. Alors $\frac{\pi(x)}{1} = 0$ donc il existe $\pi(s) \notin (p)$ tel que $\pi(sx) = 0$ soit $n \mid sx$. On en déduit que $p^\alpha \mid sx$ mais s est premier à p donc $p^\alpha \mid x$ et on a le résultat et en fait on peut même en déduire par le théorème chinois que

$$\mathbf{Z}/n\mathbf{Z} \cong \bigoplus_{p \mid n} (\mathbf{Z}/n\mathbf{Z})_{(p)}.$$

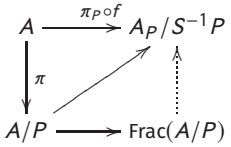
On démontre aussi que tout idéal I de $S^{-1}A$ est de la forme

$$S^{-1}J = \left\{\frac{a}{s} \ : \ a \in J, \ s \in S\right\}$$

pour un idéal J de A. On a clairement que $s^{-1}J$ est un idéal (c'est celui engendré par $f(J)$)et pour tout idéal I de $S^{-1}A$, l'ensemble

$$J = \left\{a \in A \ : \ \exists s \in S, \text{ tel que } \frac{a}{s} \in I\right\}$$

5. Je laisse à vos soins de vérifier que tout est bien défini et que tout cela correspond en réalité au diagramme commutatif suivant :



6. En effet, puisque $p \mid n$, la surjection canonique $\mathbf{Z} \longrightarrow \mathbf{Z}/p\mathbf{Z}$ passe au quotient modulo $n\mathbf{Z}$ pour donner un morphisme d'anneaux $\mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/p\mathbf{Z}$ surjectif de noyau $p\mathbf{Z}/n\mathbf{Z}$.

7. Composé de la surjection canonique $\pi : \mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z}$ et du morphisme de **4.**

est un idéal de A vérifiant $S^{-1}J = I$. En particulier, les idéaux premiers de $S^{-1}A$ s'identifient aux idéaux premiers de A ne rencontrant pas S. Les propriétés suivantes découlent facilement des définitions et de cette description des idéaux de $S^{-1}A$ pour S une partie multiplicative ne contenant pas 0 :

- Si A est intègre, alors $S^{-1}A$ est intègre [8] ;
- Si A est principal, alors $S^{-1}A$ est principal [9] ;
- Si A est factoriel, alors $S^{-1}A$ est factoriel [10].

Enfin, si on considère A un anneau et $a \in A$, alors $S = \{a^n \ : \ n \in \mathbf{N}\}$. On voit facilement que $S^{-1}A \cong A[X]/(aX-1)$ et on peut en déduire par exemple que $\mathbf{C}[X,Y]/(XY-1)$ est principal.

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 soit 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, *i.e.* $\exists x^{-1} \in A$ 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 $aa' = 1$.

Remarque : En fait, le résultat vaut toujours si l'on suppose que A est intègre et possède un nombre fini d'idéaux, alors c'est un corps. En effet, pour $x \in A \setminus \{0\}$, on a en considérant les (x^n) pour $n \in \mathbf{N}$ qu'il existe $p > q$ tels que $(x^p) = (x^q)$. En particulier, il existe $a \in A$ tel que $x^q = x^p a$ soit par intégrité $1 = x^{p-q}a$.

Exercice 4. Soit A un anneau factoriel. On suppose qu'il vérifie le théorème de Bézout, *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 $a_1, \ldots, a_n$ d'éléments de A a pour pgcd 1, alors il existe des éléments $u_1, \ldots, u_n$ de A avec $\sum_{i=1}^{n} u_i a_i = 1$.
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 $d = \text{pgcd}(a_1, \ldots, a_{n-1})$. 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 $a_1/d, \ldots, a_{n-1}/d$ donne une décomposition
$$d = u_1 a_1 + \ldots + u_{n-1} a_{n-1}, \quad u_1, \ldots, u_{n-1} \in A,$$
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 évidemment 1). Sinon I contient un élément non nul et non inversible a, qu'on peut écrire
$$a = u. \prod_{i=1}^{r} p_i^{v_i(a)},$$

8. Si $\frac{a}{s} \cdot \frac{b}{t} = 0$ alors il existe $u \in S$ tel que $uab = 0$ soit $a = 0$ ou $b = 0$ (car $0 \notin S$ par hypothèse et par intégrité de A).

9. Un tel idéal I est de la forme $S^{-1}J$ pour $J = (a)$ par principalité de A et donc $I = \left(\frac{a}{1}\right)$.

10. Commencer par établir que les inversibles de $S^{-1}A$ sont les $\frac{a}{s}$ avec a divisant un élément de S et que les irréductibles de $S^{-1}A$ sont (modulo les inversibles) les $\frac{p}{1}$ avec p irréductible de A ne divisant aucun élément de S.

avec $u \in A^\times$, $v_i(a) \in \mathbf{N}$, et les p_i irréductibles non associés deux à deux. Soit alors, pour chaque $i \in \{1, \dots, r\}$, a_i un élément de I tel que $w_i := v_i(a_i)$ soit minimum parmi les $v_i(x)$ avec $x \in I$ non nuls. Posons alors

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

Notons également μ le pgcd de $a_1, a_2, \dots, a_r, a$. Par **2.**, $\mu \in I$ et par définition des a_i, $p_i^{w_i}$ divise μ et donc $d \mid \mu$. Réciproquement, μ divise a et n'a donc pas d'autres facteurs irréductibles que $p_1, \dots, p_r$ et comme μ divise a_i pour tout i, sa valuation p_i-adique est inférieure à w_i de sorte que $\mu \mid d$ et enfin d est le pgcd de de $a_1, a_2, \dots, a_r, a$ et appartient par conséquent à I par **2**. On vérifie alors que par définition, d divise tous les éléments de I. C'est alors le plus grand car si on a un autre élément d' qui divise tous les éléments de I, alors puisque d est dans I, on aurait que d' divise d et donc d' est plus petit que d (au sens de la divisibilité), ce qui prouve que d est le plus grand diviseur commun à tous les éléments de I.

4. Soient I un idéal de A et d le pgcd de tous les éléments de I. D'après **3.**, c'est aussi le pgcd d'une famille finie $a_1, \dots, a_r$ d'éléments de I. En appliquant **2.** à $a_1/d, \dots, a_r/d$, 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.

Noter que comme en TD, on pouvait conclure directement sans passer par **3.** En effet, si $I \neq (0)$, on prend $x \in I$ l'élément dont le nombre de facteurs irréductibles (avec multiplicité) est minimal[11] parmi les éléments non nuls de I. On a alors que pour tout $a \in I$, $\mathrm{pgcd}(a, x) \mid x$ donc a moins de facteurs irréductibles que x et est dans I d'après **1.** mais donc par minimalité, $\mathrm{pgcd}(a, x) = ux$ avec $u \in A^\times$, autrement dit $x \mid a$ et $I \subseteq (x)$ tandis que l'inclusion $(x) \subseteq I$ est triviale donc $I = (x)$ et il n'est pas difficile de voir que x est le pgcd de tous les éléments de I.

On peut en revanche construire des anneaux de Bézout non principaux comme l'anneau des fonctions holomorphes étudiés dans l'exercice 7 ou certains anneaux d'entiers. Un autre exemple est donné par

$$A = \mathbf{Q}[x_i \ : \ i \in \mathbf{N}]/\langle x_i - x_{i+1}^2 \ : \ i \in \mathbf{N}\rangle.$$

En effet, soit le morphisme de $\mathbf{Q}$-algèbres injectif $\varphi_i : \mathbf{Q}[x_i] \longrightarrow A$ défini par $x_i \mapsto \overline{x_i}$ et le morphisme de $\mathbf{Q}$-algèbres injectif $\psi_i : \mathbf{Q}[x_i] \longrightarrow \mathbf{Q}[x_{i+1}]$ défini par $x_i \mapsto x_{i+1}^2$. On a alors $\varphi_{i+1} \circ \psi_i = \varphi_i$ et on pose $A_i = \varphi_i(\mathbf{Q}[x_i])$ qui est un anneau principal car isomorphe à $\mathbf{Q}[x_i]$. On a alors clairement que $A_i \subseteq A_{i+1}$ pour tout $i \in \mathbf{N}$ et $A = \bigcup_{i \in \mathbf{N}} A_i$. Il est clair que tout idéal finiment engendré de A est en fait contenu dans un A_{i_0} et est donc principal. Cela permet de démontrer que A est de Bézout. Mais, on a que l'idéal M de A engendré par toutes les $\overline{x_i}$ n'est pas principal. En effet, notons ω_i la seule racine 2^i-ième de 2 réelle positive dans $\overline{\mathbf{Q}}$ et considérons le morphisme $f : \mathbf{Q}[x_i \ : \ i \in \mathbf{N}] \longrightarrow \overline{\mathbf{Q}}$ défini par $x_i \mapsto \omega_i$. Le noyau de ce morphisme contient évidemment $\langle x_i - x_{i+1}^2 \ : \ i \in \mathbf{N}\rangle$ et donc au quotient on obtient un morphisme de A dans $\overline{\mathbf{Q}}$. Notons M' l'image de M par ce morphisme. Si maintenant M est de type fini, alors M' aussi est et on obtient un $\mathbf{Q}$-espace vectoriel de dimension finie, disons d. Ainsi tout élément de M' devrait être racine d'un polynôme à coefficients rationnels de degré au plus d mais le polynôme minimal de ω_i n'est autre que[12] $T^{2^i} - 2$ et ainsi ω_i ne peut être annulé par un polynôme de degré inférieur à 2^i, ce qui fournit bien la contradiction escomptée.

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.

11. Ce qui est bien défini puisque le nombre de facteurs irréductibles des éléments non nul est une partie non vide de $\mathbf{N}$.
12. Irréductible par Eisenstein et annulant ω_i.

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 $1 = a_1a_2 + (a_1c + ba_2 + bc)$ avec $a_1a_2 \in I_1I_2$ et $(c + ba_2 + bc) \in J$, ce qui montre que I_1I_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 :

$$a = up_1 \cdots p_r,$$

avec $u \in A^\times$ et les p_i irréductibles (non nécessairement distincts). Comme a et b sont premiers entre eux, p_i ne divise pas b, et d'après **2.**, (p_i) est étranger avec (b). D'après **1.** et par une récurrence facile, $(p_1)\ldots(p_r) = (a)$ 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 Bézout.

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 $\mathbf{Z}_p$ des entiers p-adique dans une clôture algébrique $\overline{\mathbf{Q}_p}$ de son corps des fractions $\mathbf{Q}_p$).

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

Solution. On a les deux décompositions différentes en irréductibles

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

On rappelle qu'un élément u de A est inversible si, et seulement si, $N(u) = 1$. Si $u \in A^\times$, il existe $u' \in A$ tel que $uu' = 1$ et en passant à la norme $N(u)N(u') = 1$ avec $N(u) \in \mathbf{N}$ si bien que $N(u) = 1$. Réciproquement, si $N(u) = u\overline{u} = 1$, alors[13] $\overline{u} \in A$ est l'inverse de u. En effet, 3 est irréductible car non inversible (car de norme 9) et si $3 = uu'$ avec $u, u' \in A$, alors $9 = N(3) = N(u)N(u')$ et donc $N(u), N(u') \in \{1, 3, 9\}$. Par ailleurs, si $u = a + ib$ avec $a, b \in \mathbf{Z}$, $N(u) = a^2 + 5b^2$ de sorte qu'on voit facilement qu'aucun élément n'est de norme 3. Ainsi soit $N(u)$ soit $N(u')$ vaut 1 auquel cas u ou u' est inversible et 3 est irréductible. On montre de même que $2 \pm i\sqrt{5}$ sont irréductibles.

Montrons alors que 9 et $3(2 = i\sqrt{5})$ n'ont pas de pgcd. Établissons à présent la liste des diviseurs de 9. Soit u un tel diviseur. On a alors $u' \in A$ tel que $9 = uu'$ soit $81 = N(u)N(u')$. Si $N(u) = 1$, alors[14] $u = \pm 1$ et $u' = \pm 9$. On ne peut pas avoir $N(u) = 3$ et de même $N(u) = 27$ car alors on aurait $N(u') = 3$. On peut alors avoir $N(u) = N(u') = 9$ et on voit facilement que les seuls éléments de norme 9 sont ± 3 et $\pm(2 \pm i\sqrt{5})$ et que la seule possibilité pour que le produit fasse 9 est[15] $u = u' = 3$ ou $i = \overline{u'} = 2 + i\sqrt{5}$. Enfin, si $N(u) = 81$, alors $u' = \pm 1$ et $u = \pm 9$. Finalement, les diviseurs de 9 sont (modulo les unités)

$$\mathrm{Div}(9) = \{1, 3, 2 \pm i\sqrt{5}, 9\}.$$

On procède de même avec[16] $3(2+i\sqrt{5})$. On écrit de même $3(2+i\sqrt{5}) = uu'$ avec $u, u' \in A$ et $81 = N(u)(N(u')$. Les cas $N(u) = 1$ et $N(u) = 81$ donnent ± 1 et $\pm 3(2 + i\sqrt{5})$ tandis que les cas $N(u) = 3$ ou 27 sont impossibles. Reste le cas $N(u) = N(u') = 9$ et on voit que les seules valeurs possibles de u et u' de norme 9 dont le produit vaut $3(2 + i\sqrt{5})$ sont $u = 3$ et $u' = 2 + i\sqrt{5}$ ou l'inverse. On en déduit (modulo les unités) que

$$\mathrm{Div}(3(2 + i\sqrt{5})) = \{1, 3, 2 + i\sqrt{5}, 3(2 + i\sqrt{5})\}.$$

Supposons alors qu'il existe un pgcd d à 9 et $3(2 + i\sqrt{5})$. Ce pgcd[17] est dans l'intersection des deux ensembles de diviseurs explicités plus haut donc (modulo les unités) $d \in \{1, 3, 2 + i\sqrt{5}\}$. Mais puisque $3 \mid 9, 3(2 + i\sqrt{5})$ on doit aussi avoir que $3 \mid d$ donc comme $2 + i\sqrt{5}$ et 3 sont irréductible et que 1 est inversible, $d \neq 2 + i\sqrt{5}$ et $d \neq 1$ si bien que $d = 3$. Enfin, comme $2 + i\sqrt{5} \mid 9, 3(2 + i\sqrt{5})$ on doit aussi avoir que $2 + i\sqrt{5} \mid d = 3$ ce qui est absurde car on a deux irréductibles non associés. On a donc une contradiction et ces deux éléments n'ont pas de pgcd dans A!

De même, on montre que 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm dans A. Sinon, si m est leur ppcm, alors puisque $3, 2 + i\sqrt{5} \mid 9$, on a $m \mid 9$ et de même $3, 2 + i\sqrt{5} \mid 3(2 + i\sqrt{5})$, on a $m \mid 3(2 + i\sqrt{5})$ et donc $m \in \{1, 3, 2 + i\sqrt{5}\}$ modulo les inversibles. Mais $3 \mid m$ et $2 + i\sqrt{5} \mid m$ ce qui fournit de la même façon une contradiction.

13. Car si $u = a + bi$ avec $a, b \in \mathbf{Z}$, $\overline{u} = a - bi$.

14. On voit facilement que $a^2 + 5b^2 = 1$ équivaut à $a = \pm 1$ et $b = 0$.

15. Par exemple, $3(2 + i\sqrt{5}) = 6 + 3i\sqrt{5} \neq 3$ en utilisant le fait que la famille $(1, i)$ est libre dans $\mathbf{C}$.

16. Attention qu'on ne peut pas *a priori* en déduire que les seuls diviseurs sont 1, 3, $2 + i\sqrt{5}$ et $3(2 + i\sqrt{5})$ car 3 et $2 + i\sqrt{5}$ sont irréductibles car l'anneau n'est ici **PAS** factoriel!

17. Je rappelle qu'on dit que deux éléments a et b d'un anneau intègre possèdent un pgcd s'il existe un élément $d \in A$ tel que $d \mid a, b$ et tel que pour tout $c \mid a, b$, alors $d \mid c$. Un tel élément est défini aux inversibles près. je vous renvoie page 49 du Perrin si vous désirez plus de détails.

Exercice 7. Soit $\mathcal{H}$ l'anneau des fonctions holomorphes de $\mathbf{C}$ dans $\mathbf{C}$.

1. Montrer que $\mathcal{H}$ est intègre. Quel est son corps des fractions ?
2. Montrer que $\mathcal{H}^\times$ est constitué des fonctions qui ne s'annulent pas, et que l'ensemble des irréductibles de $\mathcal{H}$ est constitué des fonctions qui ont un seul zéro avec de plus ce zéro simple.
3. Montrer que $\mathcal{H}$ 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 $\mathcal{H}$ est intègre. En effet, soient $f, g \in \mathcal{H}$ telles que $fg = 0$. Supposons que $f \neq 0$. On a alors un $z_0 \in \mathbf{C}$ tel que $f(z_0) \neq 0$ et donc par continuité un voisinage $\mathcal{V}_{z_0}$ de z_0 sur lequel f ne s'annule pas. Cela implique que g est identiquement nulle sur $\mathcal{V}_{z_0}$ qui est donc nécessairement nulle car z_0 n'est pas un isolé.
   Son corps des fractions est par définition le corps des fonctions méromorphes sur $\mathbf{C}$.
2. Si f est holomorphe et ne s'annule pas, on sait que $1/f$ est holomorphe et donc $f \in \mathcal{H}^\times$. 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 qu'il existe une fonction $g\mathcal{H}$ telle que $(z-a)g(z) = f(z)$, 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 $\mathcal{H}$, l'une des fonctions f_1, f_2 ne s'annule pas donc est dans $\mathcal{H}^\times$, 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 $a \in \mathbf{C}$.
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 $\mathcal{H}$ n'est ni factoriel ni noethérien [18].
   On peut par contre montrer que $\mathcal{H}$ vérifie le théorème de Bézout, ou encore que tout idéal *de type fini* de $\mathcal{H}$ est principal.
   Voir pour cela par exemple les notes de D. Bourqui `https://agreg-maths.univ-rennes1.fr/documentation/d`
   On peut notamment aussi y trouver un exemple explicite d'idéal qui n'est pas engendré par une partie finie, à savoir l'idéal engendré par les f_n pour $n \in \mathbf{N}$ et f_n définie pour tout $z \in \mathbf{C}$ par $f_n(z) = \frac{\sin(z)}{z(z-1)\cdots(z-n)}$.

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 $S = \{x^n \mid n \in \mathbf{N}\}$. 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 :

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

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

18. Car on rappelle qu'un anneau noethérien et intègre possède la propriété d'existence de la décomposition en produit d'irréductibles modulo les inversibles.

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 $(x+y)^{n+m} = x^n x^m + x^n x^{m-1} y + x^n x^{m-2} y^2 + \ldots + x^n y^m + x^{n-1} y^m y + \ldots + xyn + m - 1 \in I$. 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 $x^{n-1} = xx^{n-2} \in P$, donc soit $x \in P$ soit $x^{n-2} = xx^{n-3} \in P$; 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 $\phi : A \longrightarrow S^{-1}A$ 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 $\mathbf{Z}[i]$ l'anneau des entiers de Gauß.

1. Soit p un nombre premier. Montrer que p est irréductible dans $\mathbf{Z}[i]$ 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 $a^2 + b^2 \equiv 0 \pmod{p}$, 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 $\mathbf{Z}[i]$ si, et seulement si, $p \equiv 3 \bmod 4$. (Indication : on pourra calculer $(p-1)! \pmod{p}$).

Solution.

L'anneau $\mathbf{Z}[i]$ est un anneau euclidien de stathme $N : a + bi \in \mathbb{Z}[i] \mapsto a^2 + b^2 \in \mathbb{N}$. Il est facile de voir que N est multiplicative, *i.e.* si $z, z' \in \mathbf{Z}[i]$ alors $N(zz') = N(z)N(z')$. On a aussi que $z \in \mathbf{Z}[i]$ est inversible si et seulement si $N(z) = 1$. On renvoie [19] d'ailleurs aux pages 56-58 du Perrin ainsi qu'à l'exercice page 64 pour de plus amples compléments sur cet anneau des entiers de Gaußet le fait notamment qu'il est euclidien et le lien avec le fait qu'un entier n est somme de deux carrés si, et seulement si, pour tout nombre premier $p \equiv 3 \pmod 4$, alors $v_p(n)$ est paire. C'est un sujet passionnant qui donne lieu à tout un tas de questions et de problèmes encore ouverts aujourd'hui tels que (entre autres) le nombre de telles représentations comme somme de deux carrés, le nombre de points entiers dans un cercle de rayon donné ou à des généralisations à des sommes de trois, quatre ou plus de carré qui font intervenir tout une palette d'outils passionnants allant de l'algèbre, la théorie analytique des nombres ou les formes modulaires !

1. Montrons le sens direct par contraposée. Supposons qu'il existe $a, b \in \mathbf{Z}$ tel que $p = a^2 + b^2$. Alors $p = (a+ib)(a-ib)$ n'est pas irréductible car $ab \neq 0$ et donc $a \pm ib \notin \mathbf{Z}[i]^\times$.
   Réciproquement, supposons $p = uv$ avec $u, v \notin \mathbf{Z}[i]^\times$, 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 $u = u_1 + iu_2 \in \mathbf{Z}[i]$; c'est la somme de deux carrés.

19. Dont je recommande très fortement la lecture attentive, en particulier à celles et ceux qui ont l'intention de passer l'agrégation l'an prochain !

2. Soit $p \equiv 3 \pmod 4$. Soient $a, b \in \mathbf{Z}$ tels que $a^2 + b^2 \equiv 0 \pmod p$. Supposons $b \not\equiv 0 \pmod p$ alors b est inversible dans $\mathbf{Z}/p\mathbf{Z}$ et $(ab^{-1})^2 \equiv a^2(b^{-1})^2 \equiv -b^2(b^2)^{-1} \equiv -1 \pmod p$; on a aussi que $a^2 \not\equiv 0 \pmod p$ car $b^2 \not\equiv 0 \pmod p$ et $a^2 \equiv -b^2 \pmod p$. Si on pose $x = ab^{-1}$ on a alors que $x \not\equiv 0 \pmod p$ et $x^2 \equiv -1 \pmod p$; autrement dit -1 est un carré modulo p. Mais $(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$ car l'ordre de $(\mathbf{Z}/p\mathbf{Z})^\times$ est $p-1$. Donc, $\frac{p-1}{2}$ doit être pair et $p \equiv 1 \pmod 4$ ce qui est une contradiction car on supposé $p \equiv 3 \pmod 4$. On a donc montré que $b \equiv 0 \pmod p$. De même, si on suppose $a \not\equiv 0 \pmod p$ on arrive à une contradiction et $a \equiv 0 \pmod p$ aussi.

3. Pour tout entier $a \in \mathbf{Z}$ les classes possibles modulo 4 de a^2 sont : 0 ou 1 ; donc pour $a, b \in \mathbf{Z}$ les classes possibles pour $a^2 + b^2$ modulo 4 sont 0, 1 ou 2.

4. Montrons que les trois conditions suivantes sont équivalentes

(a) p est irréductible,

(b) $p \equiv 3 \pmod 4$,

(c) p n'est pas la somme de deux carrés.

On sait par **1.** que (a) et $c)$ sont équivalents. C'est facile de voir que (b) implique (c) : d'après la question **3.** si $p = a^2 + b^2$ alors $p \not\equiv 3 \pmod 4$. Montrons que (a) implique (b). Supposons p irréductible dans $\mathbf{Z}[i]$, alors par **1.** il n'est pas somme de deux carrés et donc $p \neq 2 = 1^2 + 1^2$. Supposons alors que $p \equiv 1 \pmod 4$ et montrons à l'aide du théorème de Wilson[20] qu'il existe $x \in \mathbf{Z}$ tel que $x^2 \equiv -1 \pmod p$. 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 $x - i$, ce qui est absurde car s'il existait $a, b \in \mathbf{Z}$ tels que $x + i = p(a + ib)$, on aurait $pb = 1$ ce qui n'est pas possible. Montrons alors que -1 est un carré modulmo p. En effet, p s'écrit comme $p = 2k + 1$ avec k un entier pair et on écrit $(p-1)! = 2k(2k-1)\cdots(k+1)k(k-1)\cdots 2 \times 1$ Comme pour tout $i \in \{0, \ldots, k-1\}$ on a que $2k - i \equiv -(i+1) \pmod p$, on a que

$$\begin{aligned}(p-1)! &\equiv -1 \times -2^2 \times \cdots \times \left(-(i+1)^2\right) \times \cdots \times \left(-(k-1)^2\right) \times (-k^2) \\ &\equiv (-1)^k \times 2^2 \times 3^2 \times \cdots \times (k-1)^2 \times k^2 \\ &\equiv (-1)^2 (k!)^2 \\ &\equiv -1 \pmod p\end{aligned}$$

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

Noter qu'on a en réalité l'équivalence

$$-1 \text{ est un carré dans } \mathbf{F}_p \quad \Longleftrightarrow \quad p \not\equiv 3 \pmod 4 .$$

L'implication de gauche à droite est claire par **2.**. Il est également clair que si $p = 2$, $-1 \equiv 1 \equiv 1^2 \pmod 2$. On peut donc supposer $p \equiv 1 \pmod 4$ dans la suite et on veut montrer que -1 est un carré modulo p sans recourir au théorème de Wilson. On peut le démontrer en remarquant que le morphisme $\mathbf{F}_p^\times \to \mathbf{F}_p^\times$ donné par $x \mapsto x^2$ est de noyau $\{\pm 1\}$ de sorte que l'image de ce morphisme (autrement dit les carrés de $\mathbf{F}_p^\times$) sont au nombre de $\frac{\#\mathbf{F}_p^\times}{2} = \frac{p-1}{2}$. On sait alors par le petit théorème de Fermat que pour tout $a \in \mathbf{F}_p^\times$, $a^{p-1} \equiv 1 \pmod p$ de sorte que $a^{\frac{p-1}{2}}$ est racine de $X^2 - 1 =$ dans $\mathbf{F}_p^\times$ et donc vaut 1 ou -1. Il est clair que si $a \equiv b^2 \pmod p$ est un carré, alors $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod p$. Or tout élément de $\mathbf{F}_p^\times$ est racine de $X^{p-1} - 1 = \left(X^{\frac{p-1}{2}} - 1\right)\left(X^{\frac{p-1}{2}} + 1\right)$. Comme on a $\frac{p-1}{2}$ carrés, on voit que ces carrés sont exactment les racines de[21] $X^{\frac{p-1}{2}} - 1$. Mais comme $\frac{p-1}{2}$ est paire, on voit que -1 est racine de $X^{\frac{p-1}{2}} - 1$ et est donc un carré modulo p.

Par ailleurs, pour déterminer si p est irréductible (et donc si (p) est premier puisque l'anneau est euclidien donc factoriel), on pouvait aussi raisonner comme suit. On a par définition $A = \mathbf{Z}[i] = \mathbf{Z}[X]/(X^2+1)$ et on note $\pi_A : \mathbf{Z}[X] \to A$ la surjection

20. Je rappelle que pour démontrer le théorème de Wilson, on écrit

$$(p-1)! \equiv \prod_{x \in \mathbf{F}_p^\times} x \pmod p$$

et regroupant chaque $x \neq \pm 1$ avec son inverse x^{-1} qui vérifie $x \neq x^{-1}$, on obtient que $(p-1)! \equiv 1 \times (-1) \equiv -1 \pmod p$.

21. Dans un corps commutatif, un polynôme ne peut avoir plus de racines que son degré.

canonique. Donc $\pi : \mathbf{Z}[X]/(p, X^2+1) \cong A/(p)$. En effet, on a la surjection canonique $\mathbf{Z}[X] \to \mathbf{Z}[X]/(p, X^2+1)$ de noyau l'idéal (p, X^2+1). Ainsi, ce morphisme passe au quotient modulo (X^2+1) pour fournir un morphisme surjectif $\tilde{\pi} : A = \mathbf{Z}[X]/(X^2+1) \to \mathbf{Z}[X]/(p, X^2+1)$ tel que $\tilde{\pi} \circ \pi_A = \pi$. Il est alors clair que le noyau est l'idéal engendré par (p) et qu'on obtient au quotient l'isomorphisme souhaité. De même, à partir du fait que [22] $\mathbf{Z}[X]/(p) \cong \mathbf{F}_p[X]$, on a $\mathbf{Z}[X]/(p, X^2+1) \cong \mathbf{F}_p[X]/(X^2+1)$ si bien qu'on a l'isomorphisme souhaité. Il suffit alors de voir que si -1 est un carré, disons $\alpha^2 \equiv -1 \pmod p$, modulo p (autrement dit d'après ce qui précède si $p = 2$ ou $p \equiv 1 \pmod 4$), alors $X^2+1 = (X-\alpha)(X+\alpha)$ et l'anneau $\mathbf{F}_p[X]/(X^2+1)$ n'est pas intègre et p n'est pas premier tandis que si -1 n'est pas un carré modulo p (autrement dit si $p \equiv 3 \pmod p$), alors X^2+1 n'a pas de racine dans le corps $\mathbf{F}_p$ et est de degré 2 donc irréductible et $\mathbf{F}_p[X]/(X^2+1) \cong \mathbf{F}_4$ est un corps et (p) est premier.

Exercice 10. Soit A le sous-anneau de $\mathbf{C}$ 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 $B^\times \cup \{0\}$ 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 $\mathbf{Z}[X]/P$ 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 $\mathbf{N}$.
3. Montrer que 1 et -1 sont les seuls éléments inversibles de A.
4. Montrer qu'il n'existe pas de morphisme d'anneaux de A dans $\mathbf{Z}/2\mathbf{Z}$ ou $\mathbf{Z}/3\mathbf{Z}$ (indication : pour chacun des deux cas, supposer que f soit un tel morphisme, 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 $\mathbf{Z}[x]$).
   (c) Montrer que A est principal.

Solution.

1. Supposons B euclidien et notons v sont 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 $b \in B^\times \cup \{0\}$ tel que $b + (x) = a + (x)$, *i.e.* tel que $a = qx + b$ pour $q \in B$ et b inversible. Si B est un corps, alors $x = 0$ convient. Sinon soit [23] $x \in B\backslash(B^\times \cup \{0\})$ tel que $v(x)$ soit minimal dans $B\backslash(B^\times \cup \{0\})$. 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 nul ou inversible et $\pi(b) = \pi(a)$ avec $\pi : B \to B/(x)$ la surjection canonique.
2. Puisque clairement $\alpha + \overline{\alpha} = 1$ et $\alpha\overline{\alpha} = 5$, on voit que [24] $\alpha = \frac{1+i\sqrt{9}}{2}$ est racine de $P(X) = X^2 - X + 5$. Montrons que A est isomorphe à $\mathbf{Z}[X]/(P)$. Pour tout $F \in \mathbf{Z}[X]$ il existe $Q, R \in \mathbf{Z}[X]$ tels que $F = QP + R$ où $R = 0$ ou $\deg(R) < \deg P = 2$ car le coefficient dominant de P est inversible dans [25] $\mathbf{Z}$. On peut donc définir un morphisme π de $\mathbf{Z}[X]$ dans $\mathbf{Z}[X]/(P)$ qui a F associe R, le reste de la division euclidienne de F par P. Comme $P(\alpha) = 0$ le morphisme

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

   se factorise par (P) et on obtient un morphisme $\tilde{\varphi} : \mathbf{Z}[X]/(P) \to \mathbf{Z}[\alpha]$ tel que $\varphi = \tilde{\varphi} \circ \pi$. Le morphisme $\tilde{\varphi}$ est en fait surjectif : comme $\alpha^2 = \alpha - 5$ on sait que 1 et α engendrent $\mathbf{Z}[\alpha]$. Si $R(X) \in \mathbf{Z}[X]/(P)$ 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 $\tilde{\varphi}(aX + b) = \tilde{\varphi}(a'X + b')$

22. En effet, la réduction modulo p des coefficients fournit un morphisme surjectif $\mathbf{Z}[X] \to \mathbf{F}_p[X]$ de noyau (p).
23. Bien noter que puisque B n'est pas un corps, $B\backslash(B^\times \cup \{0\}) \neq \emptyset$.
24. Ou on utilise que l'on sait que si α est racine d'un polynôme à coefficients entiers (et donc réels), alors $\overline{\alpha}$ aussi et on calcule alors $(X - \alpha)(X - \overline{\alpha})$.
25. C'est un résultat très important. Voir par exemple le lemme 3.31 du Perrin.

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

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 $\mathbf{Z}[\alpha]^*=\{-1,1\}$.

4. Supposons $f:A\to\mathbf{Z}/2\mathbf{Z}$ un morphisme d'anneaux. Puisque $f(1)=1$ et qu'on a un morphisme d'anneaux, pour tout $n\in\mathbf{Z}$, $f(n)$ n'est autre que la réduction de n modulo 2. Par ailleurs, on a dans A que $\alpha^2-\alpha+5=0$ donc donc il existe $\beta=f(\alpha)\in\mathbf{Z}/2\mathbf{Z}$ tel que $\beta^2-\beta+1=0$, or $\beta^2-\beta+1=1\neq0$ dans $\mathbf{Z}/2\mathbf{Z}$ car $x^2=x$ pour tout $x\in\mathbf{Z}/2\mathbf{Z}$. Ainsi on a une contradiction. De même si $f:A\to\mathbf{Z}/3\mathbf{Z}$ on aurait $\beta=f(\alpha)\in\mathbf{Z}/3\mathbf{Z}$ tel que $\beta^2-\beta-1=0$ mais X^2-X-1 n'a pas de racines dans $\mathbf{Z}/3\mathbf{Z}$.

5. Supposons A euclidien; d'après **1.** il existe x non inversible et non nul tel que la restriction de $\pi:A\to A/(x)$ à $A^\times\cup\{0\}$ soit surjective. Comme $A\simeq\mathbf{Z}[\alpha]$, on a $A^\times:\{-1,1\}$ et $\pi|_{A^\times\cup\{0\}}:\{-1,1,0\}\to A/(x)$ est surjective. On montre que $A/(x)$ est un corps[26] : 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 $\pi(b)=a+(x)$ est inversible d'inverse $\pi(b^{-1})$. Ainsi $A/(x)$ est donc un corps. Comme $p|_{A^\times\cup\{0\}}$ est surjective le cardinal de $A/(x)$ est inférieur ou égal à 3, $A/(x)$ est donc isomorphe soit à $\mathbf{Z}/2\mathbf{Z}$ soit à $\mathbf{Z}/3\mathbf{Z}$. On aurait donc un morphisme de A dans $\mathbf{Z}/2\mathbf{Z}$ ou dans $\mathbf{Z}/3\mathbf{Z}$, ce qui est impossible. Donc A n'est pas euclidien.

6. (a) Soient $a,b\in A$ non nuls. Soit $x=\frac{a}{b}\in\mathbf{C}$; il s'écrit $x=u+v\alpha$ avec $u,v\in\mathbf{Q}$. ($x=\frac{a\overline{b}}{b\overline{b}}=\frac{1}{N(b)}(a\overline{b})\in\mathbf{Q}[\alpha]$). Soit n la partie entière de v. Alors $v\in[n,n+1[$. Supposons[27] $v\notin\left]n+\frac13,n+\frac23\right[$ et soient s,t les entiers les plus proches de u et de v respectivement. Alors $|s-u|\leqslant\frac12$, $|t-v|\leqslant\frac13$. On pose $q=s+t\alpha$ et donc $q\in A=\mathbf{Z}[\alpha]$. On a alors que $N(x-q)=N((u-s)+(v-t)\alpha)=(s-u)^2+(s-u)(t-v)+5(t-v)^2\leq\frac14+\frac16+\frac59=\frac{35}{36}<1$. On pose $r=a-bq\in A$. On a alors que $a=bq+r$ et $N(r)<N(b)$.
Supposons maintenant $v\in\left]n+\frac13,n+\frac23\right[$. On prend $2x=2u+2v\alpha$ et $2v\in\left]2n+\frac23,2n+1+\frac13\right[$, si m est la partie entière de $2v$ alors $2v\notin\left]m+\frac13,m+\frac23\right[$. On se ramène donc au cas précédent et $2a=bq+r$ avec $N(r)<N(b)$.

(b) On a que $A\simeq\mathbf{Z}[X]/(X^2-X+5)$ donc

$$A/(2)\simeq\mathbf{Z}[X]/(2,X^2-X+5)\simeq(\mathbf{Z}/2\mathbf{Z})[X]/(X^2-X+5)\simeq\mathbf{F}_2[X]/(X^2+X+1)$$

et X^2+X+1 est irréductible dans $\mathbf{F}_2[X]$ (car de degré 2 sans racine), on a que $A/(2)$ est un corps (isomorphe à $\mathbf{F}_4$).

(c) Soit I un idéal non nul de A et $a\in I$, $a\neq0$ tel que $N(a)$ soit minimal parmi les éléments non nuls de I. 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 $a\in(2)$ et on peut supposer que $q\notin(2)$. 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 finalement bien que $I=(a)$ et A est principal.

Un autre exemple (utilisant le même critère que celui en **1.**) est donné en exercice dans le Perrin (corrigé dans *Exercices de mathématiques pour l'agrégation : Algèbre 1* de Francinou et Gianella). Il s'agit de l'anneau $\mathbf{R}[X,Y]/(X^2+Y^2+1)$ qui est principal non euclidien et constitue un bon exercice pour s'entraîner sur les anneaux de polynômes.

Exercice 11. Le *radical de Jacobson* d'un anneau commutatif A est l'intersection de tous les idéaux maximaux de A. On le note $\mathrm{rad}\,A$.

1. Soit A un anneau. Montrer qu'un élément a est dans le radical de A si, et seulement si, pour tout $x\in A$, $1-ax$ est inversible.

26. Ou alors on raisonne en termes de groupes sous-jacents.
27. Il est conseillé ici de s'aider d'un dessin!

2. Toujours en supposant que A est commutatif, montrer que si $x \in A$ est nilpotent, alors $1 - ax$ est inversible, pour tout élément $a \in A$.
3. Toujours dans le cas commutatif, montrer que le radical de A est le plus grand idéal de A tel que $1 - x$ est inversible pour tout $x \in \operatorname{rad} A$.
4. Toujours dans le cas où A est commutatif, soit I un idéal dont tous les éléments sont nilpotents. Montrer que $I \subseteq \operatorname{rad} A$.
5. Calculer le radical de $\mathbf{Z}$, $\mathbf{R}[X]$, $\mathbf{Z}/n\mathbf{Z}$ (pour un entier $n > 1$).

Solution.

1. Supposons que $a \in \operatorname{rad}(A)$ et soit $x \in A$. Si $1 - ax$ est non inversible, $1 - ax$ appartient à un idéal maximal $\mathfrak{M}$ de A. Mais par définition, $a \in \mathfrak{M}$ donc $1 = 1 - ax + ax \in \mathfrak{M}$, ce qui est absurde.
   Réciproquement, soit $a \in A$ tel que pour tout $x \in A$, $1 - ax \in A^\times$. Supposons qu'il existe un idéal maximal $\mathfrak{M}$ ne contenant pas a. Alors si $\pi : A \longrightarrow A/\mathfrak{M}$ est la surjection canonique, on a que $\pi(a) \neq 0$ et $A/\mathfrak{M}$ étant un corps et par surjectivité de π, il existe $x \in A$ tel que $\pi(a)\pi(x) = \pi(ax) = 1$ soit $1 - ax \in \mathfrak{M}$, ce qui contredit l'inversibilité de $1 - ax$. Finalement, $a \in \operatorname{rad}(A)$.
   On pouvait aussi raisonner en disant que dans ce cas $\mathfrak{M} + (a) = A$ de sorte que $1 = m + ax$ et $1 - ax = m \in \mathfrak{M}$ ne peut être inversible.
2. Supposons que $x^k = 0$ pour $k \in \mathbf{N}^\times$. On pose alors[28]
$$u = \sum_{n=0}^{+\infty} (ax)^n = \sum_{n=0}^{+\infty} a^n x^n = \sum_{n=0}^{k-1} a^n x^n$$
   qui est bien défini car x est nilpotent et A est commutatif. On a alors
$$(1 - ax)u = \sum_{n=0}^{k-1} a^n x^n - \sum_{n=1}^{k-1} a^n x^n = 1$$
   si bien que u est l'inverse de $1 - ax$ qui est donc inversible.
3. Le radical est clairement un idéal vérifiant la condition. Soit alors un idéal I tel que pour tout $y \in I$, $1 - y$ est inversible. Soit $a \in I$ et utilisons le critère de **1.** pour montrer que $a \in \operatorname{rad}(A)$. Soit $x \in A$, alors $y = ax \in I$ et donc $1 - ax = 1 - y$ est inversible, ce qui démontre le résultat.
4. C'est évident en combinant **2.** et **1.**.
5. On sait que les idéaux maximaux de $\mathbf{Z}$ sont les $p\mathbf{Z}$ avec p premier si bien que
$$\operatorname{rad}(\mathbf{Z}) = \bigcap_{p \text{ premier}} p\mathbf{Z} = \{0\}.$$
   De même, les idéaux de $\mathbf{R}[X]$ sont les idéaux engendrés par un polynôme irréductible de $\mathbf{R}[X]$ et $\operatorname{rad}(\mathbf{R}[X]) = \{0\}$. La discussion page 3 fournit que
$$\operatorname{rad}(\mathbf{Z}/n\mathbf{Z}) = \bigcap_{\substack{p \mid n \\ p \text{ premier}}} p\mathbf{Z}/n\mathbf{Z} = r(n)\mathbf{Z}/n\mathbf{Z}$$
   avec $r(n) = \prod_{p \mid n} p$ le *radical*[29] de n.

Le radical et le radical de Jacobson d'un idéal jouent un rôle important en géométrie algébrique notamment.

Exercice 12. Soit A un anneau euclidien de stathme φ. Montrer qu'il existe un stathme $\overline{\varphi}$ tel que $(A, \overline{\varphi})$ soit euclidien et pour tous a, b dans A non nuls, $\overline{\varphi}(ab) \geqslant \overline{\varphi}(a)$. Montrer alors :

1. Pour tout $a \in A \setminus \{0\}$, $\overline{\varphi}(a) \geqslant \overline{\varphi}(1)$;
2. $\overline{\varphi}(a) = \overline{\varphi}(1)$ si, et seulement si, a est inversible dans A;

28. Reconnaître la série $\frac{1}{1-ax}$.
29. Qui intervient notamment dans la célèbre conjecture *abc* qui explore le lien entre les structures additive et multiplicative des entiers.

3. Si $a, b \in A \setminus \{0\}$ sont associés, alors $\overline{\varphi}(a) = \overline{\varphi}(b)$;

4. Si $a, b \in A \setminus \{0\}$ sont tels que a divise b et $\overline{\varphi}(a) = \overline{\varphi}(b)$, alors a et b sont associés.

Montrer que tout stathme ne vérifie pas les propriétés précédentes.

On suppose maintenant que le stathme φ vérifie les propriétés suivantes

(i) Pour tous $a, b \in A \setminus \{0\}$, $\varphi(ab) = \varphi(a)\varphi(b)$;

(ii) Pour tous[30] $a, b \in A \setminus \{0\}$, $\varphi(a+b) \leqslant \max(\varphi(a), \varphi(b))$.

Montrer que A est un corps ou isomorphe à $k[X]$ pour un certain corps k.

Solution.
On considère $A = \mathbf{Z}$ muni de son stathme usuel $\varphi(n) = |n|$. L'application $\tilde{\varphi} : \mathbf{Z}^* \to \mathbf{N}$ défini par $\tilde{\varphi}(n) = 2n$ si $n > 0$ et $\tilde{\varphi}(n) = -n$ si $n < 0$. Il s'agit d'un stathme. En effet, soient $(a, b) \in \mathbf{Z} \times \mathbf{Z}^*$, il existe alors $q \in \mathbf{Z}$ et $r = 0$ ou $|r| < |b|/2$. On en déduit que si $b < 0$, alors $0 < \tilde{\varphi}(r) = 2r < -b = \tilde{\varphi}(b)$ et si $b > 0$, alors $0 < \tilde{\varphi}(r) = 2r < b < 2b = \tilde{\varphi}(b)$ si bien qu'on a bien un stathme mais $\tilde{\varphi}(-1) = 1 < \tilde{\varphi}(1) = 2$.
Soit alors (A, φ) un anneau euclidien. On pose $\overline{\varphi} : A \setminus \{0\} \to \mathbf{N}$ défini par

$$\forall a \in A \setminus \{0\}, \quad \overline{\varphi}(a) = \min_{x \in A \setminus \{0\}} \varphi(ax).$$

Montrons qu'il s'agit d'un stathme vérifiant les conditions souhaitées[31]. Soient $a \in A$ et $b \in A \setminus \{0\}$, il existe $x_0 \in A \setminus \{0\}$ tel que $\overline{\varphi}(b) = \varphi(bx_0)$. On effectue alors la division euclidienne de ax_0 par bx_0 de sorte qu'il existe q et r avec $r = 0$ ou $\varphi(r) < \varphi(bx_0) = \overline{\varphi}(b)$ tels que $ax_0 = bx_0 q + r$. On en déduit que $x_0 \mid r$ (A est euclidien donc en particulier factoriel) et $r = x_0 r'$ et par intégrité $a = bq + r'$ avec $\overline{\varphi}(r') \leqslant \overline{\varphi}(x_0 r') = \overline{\varphi}(r) < \overline{\varphi}(b)$ et on a donc bien construit un stathme.

1. C'est évident par définition de $\overline{\varphi}$ car pour $a \in A \setminus \{0\}$, il existe $x \in A \setminus \{0\}$ tel que $\overline{\varphi}(a) = \varphi(ax) \geqslant \min_{y \in A \setminus \{0\}} \varphi(y) = \overline{\varphi}(1)$.

2. Si a est inversible, il existe $a' \in A \setminus \{0\}$ tel que $aa' = 1$ et supposons que $\overline{\varphi}(1) = \varphi(x)$ pour $x \in A \setminus \{0\}$. On a alors que par définition $\overline{\varphi}(a) \leqslant \varphi(xa'a) = \varphi(x) = \overline{\varphi}(1)$ donc $\overline{\varphi}(1) = \overline{\varphi}(a)$. Réciproquement, si $\overline{\varphi}(1) = \overline{\varphi}(a)$, on effectue la division euclidienne de 1 par a et on obtient $q \in A$ et $r = 0$ ou $\overline{\varphi}(r) < \overline{\varphi}(a) = \overline{\varphi}(1)$. Or, d'après **1.**, cela implique que $r = 0$ et donc que $1 = ax$ et ainsi que a est inversible.

3. Si a et b sont associés, alors il existe $u \in A^\times$ tel que $a = bu$ et on suppose que $\overline{\varphi}(a) = \varphi(ax)$ avec $x \in A \setminus \{0\}$. On a alors que $\overline{\varphi}(b) \leqslant \varphi(bux) = \varphi(ax) = \overline{\varphi}(a)$. On obtient alors l'autre inégalité de façon similaire par symétrie et ainsi $\overline{\varphi}(a) = \overline{\varphi}(b)$.

4. On remarque que, par définition, quels que soient $a, b \in A \setminus \{0\}$, alors $\overline{\varphi}(ab) \geqslant \overline{\varphi}(a)$. Supposons alors que $a \mid b$ et que $\overline{\varphi}(a) = \overline{\varphi}(b)$. Puisque $a \mid b$, il existe $c \in A \setminus \{0\}$ tel que $b = au$. Effectuons alors la division euclidienne de a par b qui fournit l'existence de $q \in A \setminus \{0\}$ et de $r = 0$ ou $\overline{\varphi}(r) < \overline{\varphi}(b)$ donc $a = bq + r = auq + r$. On en déduit que $r = ar'$ et $1 = uq + r'$. Or, $\overline{\varphi}(r) \geqslant \overline{\varphi}(a)$ mais on a $\overline{\varphi}(r) < \overline{\varphi}(b)$ ce qui fournit une contradiction si $r \neq 0$. On en déduit que $r = 0$ et donc $r' = 0$ et $1 = uq$ si bien que u est inversible et a et b sont associés.

Parfois certains auteurs incluent dans le définition d'un stathme ces conditions et qualifient les stathmes définis dans le cours de pré-stathme. On voit que les deux définitions sont bien équivalentes.

Passons à la dernière partie de l'exercice et supposons que φ satisfasse (i) et (ii). On a donc $\varphi(1)^2 = \varphi(1)$ si bien que puisque A est intègre, $\varphi(1) = 0$ ou 1. Si $\varphi(1) = 0$, alors pour tout $a \neq 0$, $\varphi(a) = \varphi(1)\varphi(a) = 0$. Ainsi en effectuant la division euclidienne de 1 par a, il vient $1 = aq + r$ avec $r = 0$ ou $\varphi(r) = 0 < \varphi(a) = 0$ ce qui est impossible donc $r = 0$ et a est inversible. On en déduit que A est un corps. Supposons alors que $\varphi(1) = 1$. Commençons par établir que $a \neq 0$ est inversible si, et seulement si, $\varphi(a) = 1$. Si a est inversible, il existe $a' \neq 0$ tel que $aa' = 1$ donc $\varphi(a)\varphi(a') = 1$ avec $\varphi(a) \in \mathbf{N}$ de sorte que $\varphi(a) = 1$. Réciproquement, si $\varphi(a) = 1$, alors montrons que pour tout $x \neq 0$, $\varphi(x) \neq 0$. Si $\varphi(x) = 0$, alors la division euclidienne de 1 par x fournit que $1 = xx'$ et x est inversible mais alors on aurait $\varphi(x) = 1$ ce qui est absurde. En particulier, pour tout $x, y \neq 0$, on a $\varphi(xy) \geqslant \varphi(x)$ et toutes les propriétés **1.**, **2.**, **3.** et **4.** sont vérifiées. On a alors que si $\varphi(a) = 1 = \varphi(1)$, alors a est inversible. Dans ce cas, montrons que $k = A^\times \cup \{O\}$ est un corps. En effet, k est stable par mutliplication. Soient $x, y \in A^\times$, alors il existe

30. On parle de stathme ou de valuation *ultramétrique*.

31. En réalité, vous pouvez essayer de vous convaincre que si l'on souhaite ces propriétés, on n'a pas d'autre choix.

x', y' tels que $xx' = 1$ et $yy' = 1$ donc $\varphi(x)\varphi(x') = 1$ avec $\varphi(x) \in \mathbf{N}$ de sorte que $\varphi(x) = 1$ et de même $\varphi(y) = 1$. On a alors $\varphi(xy) = \varphi(x)\varphi(y) = 1$ donc $xy \in A^\times$. De même, si $x \neq -y$, on a $\varphi(x+y) \leqslant \max(1,1) = 1$ et puisque pour tout $a \neq 0$, $\varphi(a) \geqslant 1$, il vient $\varphi(x+y) = 1$ et $x + y \in A^\times$ et sinon $x + y = 0$. Comme tout élément non nul de k possède évidemment un inverse, on a ainsi bien un corps. Montrons alors que $A \cong k[X]$. Soit alors $a_0 \in A \setminus k$ de stathme minimal. On obtient alors nécessairement un élément premier par minimalité. Montrons que tout élément est de stathme une puissance de $\varphi(a_0)$. Notons tout d'abord que si $\varphi(a) < \varphi(b)$, alors $\varphi(a+b) = \varphi(b)$. En effet, une inégalité est fournie par (ii) tandis que réciproquement

$$\varphi(b) = \varphi(a + b - a) \leqslant \max(\varphi(a+b), \varphi(a)) = \varphi(a+b)$$

par définition et car $\varphi(-a) = \varphi(a)$ car -1 est une unité. Soit alors $a \notin k$ et effectuons la division euclidienne de a par a_0 pour obtenir que $a = a_0 q + r$ avec $r \in k$. On a alors $\varphi(a) = \varphi(a_0 q + r) = \varphi(a_0 q) = \varphi(a_0)\varphi(q)$ car $\varphi(r) = 1$ et on peut raisonner par récurrence.
Pour conclure, on montre par récurrence sur n que tout élément $a \neq 0$ tel que $\varphi(a) = \varphi(a_0)^n$ est un polynôme en a_0 de degré n à coefficients dans k. C'est immédiat si $n = 0$ puisqu'alors $a \in k$. Supposons alors le résultat connu pour n et que $a \neq 0$ vérifie $\varphi(a) \leqslant \varphi(a_0)^{n+1}$. Une division euclidienne par a_0 fournit l'existence de $q, r \in A \setminus \{0\}$ tels que $a = a_0 q + r$ avec $r = 0$ ou $\varphi(r) < \varphi(a_0)$ donc $r \in k$ par minimalité. Ainsi, par (ii), $\varphi(a) = \varphi(a_0)^{n+1} = \varphi(a_0 q) = \varphi(a_0)\varphi(q)$ et $\varphi(q) = \varphi(a_0)^n$. Par hypothèse de récurrence, $q = P(a_0)$ avec $P \in k[X]$ et de degré n. Il s'ensuit que $a = a_0 P(a_0) + r$ est bien un polynôme de degré $n+1$ en a_0. Il est alors immédiat de voir que $A = k[a_0] \cong k[X]$.

Exercice 13 — Anneau local. Un anneau est dit *local* s'il n'admet qu'un seul idéal maximal.

1. Montrer que A est local si, et seulement si, l'ensemble de ses éléments non inversibles est un idéal et que, dans ce cas, cet idéal est l'unique idéal maximal.
2. Montrer que A est local si, et seulement si, pour tout élément $x \in A$, $1 - x$ ou x est inversible.
3. Un élément $x \in A$ est dit *idempotent* si $x^2 = x$. Montrer que si A est un anneau local, alors ses seuls idempotents sont 0 et 1. Donner un exemple d'anneau pour lequel la réciproque est fausse.
4. Soit k un corps et $n > 0$ un entier. Montrer que $k[X]/(X^n)$ est un anneau local et donner son idéal maximal.
5. Soit p un nombre premier, montrer que la localisation $\mathbf{Z}_{(p)}$ par rapport à l'idéal premier (p) est un anneau local et donner son idéal maximal.
6. L'ensemble des *germes de fonctions continues en* 0 est l'ensemble des classes d'équivalences de couples (f, U) avec U un intervalle ouvert de $\mathbf{R}$ contenant 0 et $f : U \to \mathbf{R}$ continue, pour la relation d'équivalence définie par $(f, U) \sim (g, V)$ si, et seulement si, il existe un ouvert $W \subseteq U \cap V$ contenant 0 tel que $f_{|W} = g_{|W}$. Montrer que cet ensemble muni de la somme et du produit induits par ceux pour les fonctions continues est un anneau local et donner son idéal maximal.

Solution.

1. Supposons que A soit local et notons $\mathfrak{M}$ son idéal maximal. Alors tout $x \in A^\times$ n'est pas dans $\mathfrak{M}$ car $\mathfrak{M} \neq A$ et si $x \in A \setminus A^\times$, alors d'après le cours [32], x est contenu dans un idéal maximal de A, donc $x \in \mathfrak{M}$ et finalement $\mathfrak{M}$ est bien l'ensemble des éléments non inversibles qui forment donc un idéal maximal. Réciproquement, soit $\mathfrak{M}$ l'idéal formé de tous les éléments non inversibles de A. Soit $\mathfrak{M}'$ un idéal maximal de A. Puisque tout élément de $\mathfrak{M}'$ est non inversible, $\mathfrak{M}' \subseteq \mathfrak{M}$ et par maximalité $\mathfrak{M}' = \mathfrak{M}$ si bien que $\mathfrak{M}$ est l'unique idéal maximal de A et A est local.
2. Supposons que A est local et soit $x \in A$. Si x et $1 - x$ ne sont pas inversibles, alors $1 = x + 1 - x$ appartient à l'idéal maximal de A (qui est l'ensemble des éléments non inversibles d'après **1.**), ce qui est absurde. Réciproquement, supposons que pour tout $x \in A$, x ou $1 - x$ est inversible. Supposons que A possède deux idéaux maximaux distincts $\mathfrak{M}$ et $\mathfrak{M}'$. On a alors un morphisme surjectif $\pi : A \to A/\mathfrak{M} \cap \mathfrak{M}'$. On a alors par le théorème chinois que [33] $A/\mathfrak{M} \cap \mathfrak{M}' \cong A/\mathfrak{M} \times A/\mathfrak{M}'$ et ainsi il existe un élément $x \in A$ tel que $\pi(x) = (0,1)$, autrement dit $x \in \mathfrak{M}$ et $1 - x \in \mathfrak{M}'$ et en particulier ni x ni $1 - x$ n'est inversible ce qui est absurde et A possède donc un unique idéal maximal.

   On pouvait aussi raisonner comme suit. Soit $\mathfrak{M}$ un idéal maximal et $y \in A \setminus \mathfrak{M}$. On a alors $A = \mathfrak{M} + (y)$ et donc $1 = ay + m$ et $ay = 1 - m$ est inversible car m ne l'est pas puisque dans $\mathfrak{M}$. Ainsi, $(y) = A$ et y est inversible. On a donc $A/\mathfrak{M} = A^\times$ et on a un unique idéal maximal qui est l'ensemble des éléments non inversibles donc A est local.

32. Ce résultat utilise le lemme de Zorn.
33. On peut établir que si I et J sont deux idéaux tels que $I + J = A$, alors $A/I \cap J = A/IJ \cong A/I \times A/J$.

3. Si A est local et $x^2 = x$ alors $x(1-x) = 0$ mais x ou $1-x$ est inversible donc $x = 1$ ou $x = 0$ et ces deux éléments conviennent. Dans l'anneau intègre $\mathbf{Z}$, les seuls idempotents sont bien 0 et 1 mais pourtant l'anneau n'est pas local car il possède une infinité d'idéaux maximaux.
4. Il est clair que les inversibles de $A = k[X]/(X^n)$ sont les $\pi(P)$ avec $P(0) \neq 0$ et où $\pi : k[X] \to A$. En effet, le fait qu'un tel polynôme soit inversible découle du fait qu'il soit premier à X^n d'une relation de Bézout tandis que si $X \mid P$, alors P est un diviseur de 0 non nul, par conséquent non inversible. Ainsi, l'ensemble des éléments non inversibles de A n'est autre que l'idéal engendré par la classe de X et A est local.
   On pouvait aussi raisonner en disant que les idéaux de $k[X]/(X^n)$ sont de la forme $(X^n) \subseteq (P)$ donc de la forme (X^k) avec $k \leqslant n$. On a donc la suite d'idéaux
   $$(X^n) \subseteq (X^{n-1}) \subseteq \cdots \subseteq (X)$$
   et on a un unique idéal maximal qui est (X).
5. On l'a vu dans l'exercice 2.
6. On vérifie aisément qu'on a une relation d'équivalence et qu'un élément est inversible si, et seulement si, $f(0) \neq 0$. Autrement dit, l'ensemble des éléments non inversibles est l'idéal formé par les classes de fonctions s'annulant en 0 et l'anneau est local.

Les anneaux locaux sont essentiels en géométrie et en théorie des nombres et tirent leur nom du fait de la dernière question qui permet d'étudier des fonctions localement autour d'un point.

Exercice 14 — Anneau de valuation discrète. Un anneau est dit *de valuation discrète* s'il est principal et n'admet qu'un seul idéal maximal $\mathfrak{M} = (\pi)$, celui-ci étant non nul.

1. Montrer que π est un élément premier de A et que tout élément premier est associé à π.
2. Montrer que tout idéal non nul de A s'écrit (π^n) pour un certain $n \in \mathbf{N}$.
3. Soit $x \in A \setminus \{0\}$. On pose $v(x) = \max\{n \in \mathbf{N} \ : \ x \in (\pi^n)\}$. Par convention, on pose $v(0) = \infty$. Montrer que v vérifie les propriétés suivantes :
   (i) Pour tout $a \in A$, $v(a) = \infty$ si, et seulement si, $a = 0$;
   (ii) Pour tous $a, b \in A$, $v(ab) = v(a) + v(b)$;
   (iii) Pour tous $a, b \in A$, $v(a+b) \geqslant \min(v(a), v(b))$.
   Montrer de plus que pour tout $a \in A$, $v(a) = 0$ si, et seulement si, a est inversible.
4. Soit K le corps de fractions de A. Montrer que l'on peut étendre v à une fonction définie sur K en posant $v\left(\frac{x}{y}\right) = v(x) - v(y)$ et que cette fonction respecte les conditions (i), (ii) et (iii) de **3**.
5. Montrer que $A = \{z \in K \ : \ v(z) \geqslant 0\}$.
6. Montrer que tout anneau de valuation discrète est euclidien.
7. Soit p un nombre premier, montrer que la localisation $\mathbf{Z}_{(p)}$ par rapport à l'idéal premier (p) est un anneau de valuation discrète.

Solution.

1. Un idéal maximal étant premier, on a évidemment que π est premier. Soit alors π' un élément premier de A. L'idéal engendré par π' est contenu dans un idéal maximal, qui est nécessairement (π) donc $\pi \mid \pi'$ et comme π' est premier donc irréductible (en effet A est en particulier factoriel car principal), π et π' sont associés.
2. Soit I un idéal de A non nul. Comme A est principal, il existe $a \in A$ tel que $I = (a)$. Par factorialité, on peut écrire $a = u\pi^n$ avec u inversible et $n \in \mathbf{N}$ car π est l'unique élément premier aux unités près et $I = (\pi^n)$.
3. Si $a = 0$, par définition, $v(a) = \infty$ et si $a \neq 0$, on écrit $a = u\pi^n$ avec u inversible et $n \in \mathbf{N}$ et $v(a) = n < \infty$.
   On écrit alors $a = u\pi^n$ avec u inversible et $n \in \mathbf{N}$ et $b = v\pi^m$ avec v inversible et $m \in \mathbf{N}$ de sorte que $ab = uv\pi^{n+m}$ et $v(a) + v(b) = n + m = v(ab)$.
   On écrit alors $a = u\pi^n$ avec u inversible et $n \in \mathbf{N}$ et $b = v\pi^m$ avec v inversible et $m \in \mathbf{N}$ de sorte que $v(a) = n$ et $v(b) = m$. Ainsi, $a+b = \pi^{\min(n,m)}(u\pi^{n-\min(n,m)} + v\pi^{m-\min(n,m)})$ si bien que $\pi^{\min(n,m)} \mid a+b$ et $v(a+b) \geqslant \min(n,m) = \min(v(a), v(b))$.
   On a alors que $v(a) = 0$ si, et seulement si, la décomposition de a est de la forme $a = u$ avec u inversible, ce qui fournit le résultat.

4. Il est facile de voir que cela définit une application $K \longrightarrow \mathbf{Z}$ et que $v\left(\frac{x}{y}\right) = \infty$ si, et seulement si, $v(x) = \infty$ soit si, et seulement si, $x = \frac{x}{y} = 0$.
On a alors si $a = \frac{x}{y}$ et $b = \frac{z}{t}$ avec $a, b \in A$ et $y, t \in A \setminus \{0\}$, que $v(ab) = v(x) + v(z) - v(y) - v(t) = v(a) + v(b)$.
Enfin, on a naturellement que si $a = \frac{x}{y}$ et $b = \frac{z}{t}$ avec $a, b \in A$ et $y, t \in A \setminus \{0\}$, alors $a + b = \frac{xt+yz}{yt}$ de sorte que $v(a + b) = v(xt + yz) - v(yt) = v(xt + yz) - v(y) - v(t)$. Par ailleurs, en utilisant **3.**, il vient que

$$v(xt + yz) \geqslant \min(v(xt), v(yz)) = \min(v(x) + v(y), v(y) + v(z))$$

si bien que $v(a + b) \geqslant \min(v(x) + v(t), v(z) - v(t)) = \min(v(a), v(b))$.

5. On a clairement que si $v(z) \geqslant 0$, alors $z = \frac{x}{y}$ avec $v(x) \geqslant v(y)$. Autrement dit $x = u\pi^{v(x)}$ et $y = v\pi^{v(y)}$ avec u, v inversibles et par conséquent $y \mid x$ et $z \in A$. Réciproquement, tout élément de A a une valuation positive par définition.

6. Soient $a = u\pi^n$ et $b = v\pi^m$ dans A avec u et v inversibles et $m, n \in \mathbf{N}$. Si $n < m$, alors $a = 0 \times b + a$ avec $v(a) = n < v(b)$ tandis que si $n \geqslant m$, alors $a = bv^{-1}u\pi^{n-m} + 0$ et on a donc bien une division euclidienne de stathme v qui rend l'anneau A euclidien.

7. C'est un anneau local d'après les exercices 2 et 13 si bien qu'il suffit de montrer qu'il est principal. Mais d'après les compléments de la page 2, puisque $\mathbf{Z}$ est principal, le localisé $\mathbf{Z}_{(p)}$ l'est. On en déduit le résultat.

Ces anneaux sont essentiels en théorie des nombres.