Feuille TD 2 – Exercices Algèbre – Anneaux – Corrigé

1 Généralités

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.
On pouvait aussi considérer pour $x \in A \setminus \{0\}$ les éléments x^n pour $n \in \mathbf{N}$. Cela est motivé par le fait que dans un groupe fini de cardinal m, $x^m = e$ et l'inverse de x est alors une puissance de x. Comme A est fini, par principe des tiroirs, il existe $n' > n$ tels que $x^{n'} = x^n$ soit $x^n(1 - x^{n'-n}) = 0$ et par intégrité, puisque $x \neq 0$, il vient $1 = x \times x^{n'-n-1}$ et on a bien que x est inversible d'inverse $x^{n'-n-1}$. Noter qu'on a bien $n' - n - 1 \geqslant 0$.

Exercice 2.

1. Montrer qu'un anneau A est un corps si, et seulement si, l'ensemble de ses idéaux a exactement deux éléments.
2. Plus généralement, montrer que si l'on suppose que A est intègre et possède un nombre fini d'idéaux, alors c'est un corps.

Solution.

1. 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, autrement dit il existe $x^{-1} \in A$ 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 $aa' = 1$.
2. 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 $1 = x^{p-q}a$. Noter qu'on a toujours $(x^p) \subseteq (x^q)$ de sorte que l'égalité $(x^p) = (x^q)$ nous apprend vraiment que $(x^q) \subseteq (x^p)$ soit qie $x^q \in (x^p)$.

Exercice 3. Soient A un anneau et I, J deux idéaux de A. On note

$$I + J = \{i + j \ : \ (i, j) \in I \times J\}$$

et IJ l'idéal engendré par les ij avec $(i, j) \in I \times J$.

1. Montrer que $I + J$ et IJ sont des idéaux de A et que $IJ \subseteq I \cap J$. Donner un exemple où l'inclusione st stricte et un exemple où on a égalité.
2. Montrer que si $I + J = A$, alors $IJ = I \cap J$.

Solution.

1. On a clairement que $(I + J, +)$ est un sous-groupe de $(A, +)$ car $0 \in I, J$ et donc $0 = 0 + 0 \in I + J$ et si $i + j \in I + J$ et $i' + j' \in I + J$ avec $i, i' \in I$ et $j, j' \in J$, alors

   $$(i + j) - (i' + j') = (i - i') + (j - j') \in I + J \quad \text{car} \quad i - i' \in I \text{ et } j - j' \in J.$$

   Par ailleurs, si $a \in A$,

   $$a(i + j) = ai + aj \in I + J \quad \text{car} ai \in I \text{ et } aj \in J$$

   car I et J sont des idéaux donc $I + J$ est bien un idéal.
   Pour IJ, on a qu'un élément de IJ est de la forme

   $$\sum_{k=1}^{s} a_k i_k j_k \quad \text{pour} \quad k \in \mathbf{N}, \quad a_k \in A, \quad i_k \in I, \quad j_k \in J.$$

   On vérifie alors sans peine que cet ensemble contient 0, est stable par somme et passage à l'opposé et absorbant de sorte que IJ est un idéal de A contenant tous les ij pour $i \in I$ et $j \in J$. Par ailleurs, tout idéal de A contenant tous ces produits, contient tous les

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 !

éléments de cette forme si bien qu'on a bien l'idéal engendré par les ij pour $i \in I$ et $j \in J$.

On n'a en général pas stabilité par somme dans l'ensemble[3] $\{ij \ : \ (i,j) \in I \times J\}$. Il est alors clair que tout élément de IJ s'écrit comme une somme finie de termes de la forme ij avec $i \in I$ et $j \in J$. Puisque I et J sont des idéaux, il est clair que $ij \in I \cap J$ et on a clairement le résultat. Dans $\mathbf{Z}$, on vérifie que si $I = n\mathbf{Z}$ et $J = m\mathbf{Z}$, alors $IJ = nm\mathbf{Z}$ et $I \cap J = \text{ppcm}(n,m)\mathbf{Z}$. On obtient en particulier égalité si n et m sont premiers entre eux et une inclusion stricte sinon.

2. Supposons que $I + J = A$, alors il s'agit de montrer qu vu de la question précédente que $I \cap J \cap IJ$. Soit $x \in I \cap J$. Par ailleurs, $1 \in A = I + J$ de sorte que $1 = i + j$ avec $i \in I$ et $j \in J$. On a alors

$$x = 1 \cdot x = (i+j)x = ix + jx \in IJ \text{car} xi ß I \text{ et } xj \in J.$$

On a donc le résultat.

Exercice 4.

1. Montrer que l'image réciproque d'un idéal premier par un morphisme d'anneaux reste un idéal premier.
2. Le résultat précdent reste-t-il valable pour un idéal maximal ? Et si le morphisme est surjectif ?
3. Montrer que dans un anneau principal, tout idéal premier non nul est maximal. Décrire les idéaux premiers et maximaux de $\mathbf{Z}$.
4. Soit A un anneau intègre qui n'est pas un corps. Montrer que $p \in A$ est irréductible si, et seulement si, (p) est maximal dans l'ensemble des idéaux principaux de A privé de A.

Solution.

1. Soit $f : A \to A'$ un morphisme d'anneaux et $\mathfrak{P}'$ un idéal premier de A'. On veut montrer que $\mathfrak{P} = f^{-1}(\mathfrak{P}')$ est un idéal premier de A. Pour cela deux méthodes. On peut utiliser que $A'/\mathfrak{P}'$ est intègre et montrer que $A/\mathfrak{P}$ l'est. On note $\pi' : A' \to A'/\mathfrak{P}'$ la surjection canonique. On a alors un morphisme $\pi' \circ f : A \to A'/\mathfrak{P}'$ tel que $\mathfrak{P} = \text{Ker}(\pi' \circ f)$. En effet, il est clair que $x \in \text{Ker}(\pi' \circ f)$ si, et seulement si, $\pi'(f(a)) = 0$ soit si, et seulement si, $f(a) \in \mathfrak{P}'$ soit si, et seulement si, $a \in \mathfrak{P} = f^{-1}(\mathfrak{P}')$. On a donc au quotient un morphisme injectif $A/\mathfrak{P} \to A'/\mathfrak{P}'$ qui permet d'identifier $A/\mathfrak{P}$ à un sous-anneau de l'anneau intègre $A'/\mathfrak{P}'$ et par conséquent $A/\mathfrak{P}$ est intègre et $\mathfrak{P}$ est bien un idéal premier.
   On peut aussi utiliser la seconde définition d'un idéal premier, à savoir que $\mathfrak{P} \neq A$ et que si $ab \in \mathfrak{P}$, alors $a \in \mathfrak{P}$ ou $b \in \mathfrak{P}$. Si on suppose par l'absurde que $\mathfrak{P} = A$, alors $1 \in f^{-1}(\mathfrak{P}')$ de sorte que $f(1) = 1 \in \mathfrak{P}'$ et $\mathfrak{P}' = A'$, ce qui est en contradiction avec le fait que $\mathfrak{P}'$ soit un idéal premier. On a donc $\mathfrak{P} \neq A$ et soient $a, b \in A$ tels que $ab \in \mathfrak{P}$. On a alors par définition et car f est un morphisme d'anneaux, $f(ab) = f(a)f(b) \in \mathfrak{P}'$ et $\mathfrak{P}'$ est premier donc $f(a)$ ou $f(b)$ est dans $\mathfrak{P}'$ soit a ou b est dans $\mathfrak{P}$, ce qui montre bien que $\mathfrak{P}$ est un idéal premier de A.
2. C'est faux pour un idéal maximal comme on le voit avec l'injection naturelle $\mathbf{Z} \to \mathbf{Q}$. En revanche, si f est surjective, le même raisonnement que ci-dessus garantit que $\pi' \circ f$ est surjective et par conéquent on obtient au quotient un isomorphisme $A/\mathfrak{P} \cong A'/\mathfrak{P}'$ si bien que $A/\mathfrak{P}$ est un corps dès que $A'/\mathfrak{P}'$ en est un.
   On pouvait aussi raisonner avec la seconde définition et montrer comme ci-dessus que si $\mathfrak{M}'$ est un idéal maximal de A' et $\mathfrak{M} = f^{-1}(\mathfrak{M}')$, alors $\mathfrak{M} \neq A$. Par ailleurs, soit I un idéal de A tel que $\mathfrak{M} \subseteq I$. On a alors, puisque f est surjective que $\mathfrak{M}' \subseteq f(I)$. Comme $\mathfrak{M}'$ est maximal dans A', on a $f(I) = \mathfrak{M}'$ ou $f(I) = A'$. Dans le premier cas, $I \subseteq f^{-1}(f(I)) = \mathfrak{M}$ donc $I = \mathfrak{M}$. Soit on a $f(I) = A'$ et alors pour tout $a \in A$, $f(a) \in A' = f(I)$ et il existe $i \in I$ tel que $f(a) = f(i)$ soit $a - i \in f^{-1}(0) \subseteq f^{-1}(\mathfrak{M}') = \mathfrak{M} \subseteq I$. On en déduit que $a \in I$ car $i \in I$ et donc $I = A$. On a donc bien que $\mathfrak{M}$ est maximal.
3. Soit A un anneau principal et $\mathfrak{P}$ un idéal premier non nul. Montrons que $\mathfrak{P}$ est maximal. Puisque $\mathfrak{P}$ est premier, $\mathfrak{P} \neq A$ et puisque A est principal, il existe $p \in A$ non nul (car $\mathfrak{P}$ est non nul) tel que $\mathfrak{P} = (p)$. Montrons que $\mathfrak{P}$ est maximal en supposant qu'il existe un idéal I tel que $\mathfrak{P} \subseteq I$. Comme A est principal, il existe $a \in A$ tel que $I = (a)$. On a donc $(p) \subseteq (a)$ soit il existe $u \in A$ tel que $p = au \in \mathfrak{P}$. Or, $\mathfrak{P}$ est premier donc $a \in \mathfrak{P}$ ou $u \in \mathfrak{P}$. Si $a \in \mathfrak{P}$, alors $(a) \subseteq (p)$ et $I = \mathfrak{P}$. Si en revanche, $u \in \mathfrak{P}$, il existe $v \in A$ tel que $u = pv$ et de $p = au$, on tire que $p = pav$. Par intégrité de A (qui est principal donc itnègre), $1 = av$ et $a \in A^\times$ de sorte que $I = (a) = A$. On a donc bien que $\mathfrak{P}$ est maximal.
   Les idéaux premiers de $\mathbf{Z}$ sont $\{0\}$ et les $p\mathbf{Z}$ pour p premiers tandis que ses idéaux maximaux sont les $p\mathbf{Z}$ pour p premiers. De même, lorsque k est un corps, les idéaux premiers de $k[X]$ sont les (P) avec $P \in k[X]$ irréductible et $\{0\}$ et les iéaux premiers de $k[X]$ sont les (P) avec $P \in k[X]$ irréductible.
4. Soit A un anneau intègre qui n'est pas un corps. Soit $p \in A$ irréductible. Supposons qu'il existe $a \in A$ tel que $(p) \subseteq (a)$. Le même raisonnement qu'en question précédente garantit que $a \in A^\times$ ou $a \in (p)$ de sorte que $(p) = (a)$ ou $(a) = A$.
   Réciproquement, soit $p \in A$ tel que (p) soit maximal dans l'ensemble des idéaux principaux de A privé de A. Montrons que p est irréductible. On écrit $p = uv$ avec $u, v \in A$. On a alors $(p) \subseteq (u)$ et par conséquent, soit $(u) = (p)$ auquel cas (par intégreité) $v \in A^\times$ soit $(u) = A$ auquel cas $u \in A^\times$. On en conclut donc bien que p est irréductible.

3. Par exemple dans $k[X,Y]$ avec k un corps, $I = (X,Y)$ et $J = (X^2, Y)$, on a que

$$X \times X^2 + Y \times Y = X^3 + Y^2$$

n'est pas de la forme $(PX + QY)(RX^2 + SY)$ car $X^3 + Y^2$ est irréductible (par exemple car il l'est sur $k(X)[Y]$ sur lequel il est de degré 2 sans racine).

Exercice 5.

1. Soient $\mathfrak{P}$ un idéal premier de A et $I_1, \dots, I_n$ des idéaux de A. On suppose que $I_1 I_2 \cdots I_n \subseteq \mathfrak{P}$. Montrer que $\mathfrak{P}$ contient l'un des I_k.
2. Montrer que si I est un idéal non premier, il existe des idéaux I_1, I_2 tels que $I \subseteq I_1$, $I \subseteq I_2$, $I_1, I_2 \neq I$ et $I_1 I_2 \subseteq I$.

Solution.

1. On raisonne par l'absurde. Si non, pour tout $k \in \{1, \dots, n\}$, il existe $x_k \in I_k$, $x_k \notin \mathfrak{P}$. On a alors

$$x_1 x_2 \cdots x_n \in I_1 I_2 \cdots I_n \subseteq \mathfrak{P}$$

de sorte que par caractère premier de $\mathfrak{P}$, il existe un $i_0 \in \{1, \dots, n\}$ tel que $x_{i_0} \in \mathfrak{P}$, ce qui est absurde.

2. Soit I un idéal non premier. Il existe ainsi $x, y \in A$ tel que $x, y \notin I$ et $xy \in I$. On pose alors $I_1 = I + (x)$ et $I_2 = I + (y)$. Puisque $x, y \notin \mathfrak{P}$, I_1 et I_2 contiennent I strictement et montrons que $I_2 I_2 \subseteq I$. Un élément de $I_2 I_2$ est de la forme

$$\sum_{i=1}^{r} a_i n_i m_i \quad r \in \mathbf{N}, \quad a_1, \dots, a_r \in A, \quad n_1, \dots, n_r \in I_1, \quad m_1, \dots, m_r \in I_2.$$

On voit donc qu'il suffit de montrer par les propriétés des idéaux que le produit d'un élément de I_1 par un élément de I_2 est dans I. Un élément de I_1 est de la forme $i + ax$ avec $i \in I$ et $a \in A$ et un élément de I_2 est de la forme $j + by$ avec $j \in I$ et $b \in A$ de sorte que

$$(i + ax)(j + by) = ij + iby + jax + ab(xy) \in I$$

car $i, j \in I$ et I est un idéal et $xy \in I$.

Exercice 6.

1. Soit $m \in \mathbf{N}$ et $m \mid n$. On pose

$$f : \left\{ \begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})^\times & \longrightarrow & (\mathbf{Z}/m\mathbf{Z})^\times \\ \overline{x}^n & \longmapsto & \overline{x}^m. \end{array} \right.$$

Montrer qu'il s'agit d'un morphisme de groupes surjectif.
On pourra commencer par traiter le cas des puissances d'un nombre premier.

2. Résoudre $7x = 2$ dans $\mathbf{Z}/37\mathbf{Z}$. Puis résoudre $10x = 6$ dans $\mathbf{Z}/34\mathbf{Z}$.
3. Résoudre le système suivant sur $\mathbf{Z}/18\mathbf{Z}$:

$$\left\{ \begin{array}{l} 2x + 3y = 1 \\ 3x + 4y = 2. \end{array} \right.$$

4. Résoudre $x^2 + x + 7 = 0$ dans $\mathbf{Z}/13\mathbf{Z}$ puis $x^2 - 4x + 3 = 0$ dans $\mathbf{Z}/12\mathbf{Z}$.

Solution.

1. n écrit

$$m = \prod_{i=1}^{r} p_i^{\beta_i} \quad \text{et} \quad n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

pour des nombres premiers distincts $p_1, \dots, p_r$ et des entiers positifs $\beta_i \leqslant \alpha_i$. Le théorème chinois garantit alors que

$$(\mathbf{Z}/n\mathbf{Z})^\times \cong \prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times \quad \text{et} \quad (\mathbf{Z}/m\mathbf{Z})^\times \cong \prod_{i=1}^{r} \left(\mathbf{Z}/p_i^{\beta_i}\mathbf{Z}\right)^\times.$$

L'isomorphisme étant donné, si on dispose pour tout i de l'inverse p_i' de $\frac{n}{p_i^{\alpha_i}}$ modulo $p_i^{\alpha_i}$ (qui existe car ces deux entiers sont premiers entre eux et que l'on peut calculer par l'algorithme de Bézout étendu) et de même de l'inverse q_j' de $\frac{n}{q_j^{\gamma_j}}$ modulo $q_j^{\gamma_j}$ par

$$\left\{ \begin{array}{ccc} (\mathbf{Z}/n\mathbf{Z})^\times & \longrightarrow & \displaystyle\prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times \\ \overline{x}^n & \longmapsto & \left(\overline{x}^{p_1^{\alpha_1}}, \dots, \overline{x}^{p_r^{\alpha_r}}\right) \end{array} \right.$$

de réciproque

$$\left\{ \begin{array}{ccc} \displaystyle\prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times & \longrightarrow & (\mathbf{Z}/n\mathbf{Z})^\times \\ \left(\overline{x_1}^{p_1^{\alpha_1}}, \dots, \overline{x_r}^{p_r^{\alpha_r}}\right) & \longmapsto & \overline{\sum_{i=1}^{r} x_i p_i' \frac{n}{p_i^{\alpha_i}}}^n \end{array} \right.$$

et de même pour $(\mathbf{Z}/n\mathbf{Z})^\times$. Ainsi, à travers ces isomorphismes, l'application $(\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/m\mathbf{Z})^\times$ devient

$$\begin{cases} \prod_{i=1}^r (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times & \longrightarrow & \prod_{i=1}^r \left(\mathbf{Z}/p_i^{\beta_i}\mathbf{Z}\right)^\times \\ \left(\overline{x_1}^{p_1^{\alpha_1}}, \dots, \overline{x_r}^{p_r^{\alpha_r}}\right) & \longmapsto & \left(\overline{x_1 p_1' \frac{n}{p_1^{\alpha_1}}}^{p_1^{\beta_1}}, \dots, \overline{x_r p_r' \frac{n}{p_r^{\alpha_r}}}^{p_r^{\beta_r}}\right) = \left(\overline{x_1}^{p_1^{\beta_1}}, \dots, \overline{x_r}^{p_r^{\beta_r}}\right). \end{cases}$$

Il suffit donc de démontrer la surjectivité de cette application ci-dessus. On considère donc un élément $\left(\overline{x_1}^{p_1^{\beta_1}}, \dots, \overline{x_r}^{p_r^{\beta_r}}\right)$ dans $\prod_{i=1}^r \left(\mathbf{Z}/p_i^{\beta_i}\mathbf{Z}\right)^\times$. Cela implique en particulier que x_i est premier à p_i et donc en particulier que $x_i \in (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times$ (c'est l'avantage de s'être ramené à des puissances de nombres premiers !) et ainsi un antécédent est donné par $\left(\overline{x_1}^{p_1^{\alpha_1}}, \dots, \overline{x_r}^{p_r^{\alpha_r}}\right)$ et on a gagné ! Pour vous faire un peu mieux une idée de ce qu'il se passe, on peut traiter le cas de $n = 24$ et $m = 4$ de sorte que l'application $(\mathbf{Z}/24\mathbf{Z})^\times \to (\mathbf{Z}/4\mathbf{Z})^\times$ de sorte que l'application correspondante (via le théorème chinois) devient

$$\begin{cases} (\mathbf{Z}/8\mathbf{Z})^\times \times (\mathbf{Z}/3\mathbf{Z})^\times & \longrightarrow & (\mathbf{Z}/4\mathbf{Z})^\times \\ \left(\overline{x}^8, \overline{y}^3\right) & \longmapsto & \overline{x}^4. \end{cases}$$

On peut alors relever $3 \in (\mathbf{Z}/4\mathbf{Z})^\times$ par $\left(\overline{3}^8, \overline{1}^3\right) \in (\mathbf{Z}/8\mathbf{Z})^\times$. Pour savoir à quel élément cela correspond pour notre problème de départ (à savoir dans $(\mathbf{Z}/24\mathbf{Z})^\times$), on sait que $3 \times 3 - 8 = 1$ de sorte que l'isomorphisme $(\mathbf{Z}/8\mathbf{Z})^\times \times (\mathbf{Z}/3\mathbf{Z})^\times \to (\mathbf{Z}/24\mathbf{Z})^\times$ est donné par $\left(\overline{x}^8, \overline{y}^3\right) \mapsto \overline{9x - 8y}^{24}$ et un antécédent de 3 (qui n'est pas premier à 24) est alors donné par $9 \times 3 - 8 = 19$ qui est bien inversible modulo 24 (car premier à 24) et vérifie que $19 \equiv 3 \mod 4$. On ne pouvait pas raisonner de même avec m et $\frac{n}{m}$ car ces deux entiers ne sont pas nécessairement premiers entre eux.

2. On remarque que 7 est premier avec 37 donc inversible dans $\mathbf{Z}/37\mathbf{Z}$. On obtient en utilisant l'algorithme d'Euclide étendu que $7 \times 16 - 3 \times 37 = 1$ de sorte que $7 \times 16 \equiv 1 \pmod{37}$. L'équation $7x = 2$ équivaut donc à $x = 16 \times 2 = 32$ modulo 37.
Ici, 10 n'est pas premier avec 34. On ne peut donc pas calculer directement son inverse. Mais, on cherche à résoudre $10x \equiv 6 \pmod{34}$ qui équivaut à $5x \equiv 3 \pmod{17}$. Ici, 5 est inversible dans $\mathbf{Z}/17\mathbf{Z}$ et $7 \times 5 - 17 \times 2 = 1$ donc l'inverse de 5 est 7 modulo 17 et $5x \equiv 3 \pmod{17}$ équivaut à $x \equiv 21 \equiv 4 \pmod{17}$. Finalement, on cherche donc les x modulo 34 tels que $x \equiv 4 \pmod{17}$, soit $x = 4, 21$.

3. Commençons par une remarque. Soient n et m deux entiers naturels premiers entre. L'isomorphisme chinois garantit que $\mathbf{Z}/nm\mathbf{Z}$ est isomorphe à $\mathbf{Z}/n\mathbf{Z} \times \cdots \times \mathbf{Z}/m\mathbf{Z}$ via

$$\varphi : \begin{cases} \mathbf{Z}/(n_1 \cdots n_r)\mathbf{Z} & \longrightarrow & \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z} \\ \overline{x}^{nm} & \longmapsto & (\overline{x}^n, \overline{x}^m) \end{cases}$$

On va alors montrer que si n_1 et n_2 sont premiers entre eux et si $f_1, \dots, f_r \in \mathbf{Z}[X_1, \dots, X_n]$, les ensembles

$$E := \{x_1, \dots, x_n \in \mathbf{Z}/n_1n_2\mathbf{Z} \ : \ f_1(x_1, \dots, x_n) \equiv \cdots \equiv f_r(x_1, \dots, x_n) \equiv 0 \pmod{n_1n_2}\}$$

et

$$F := \prod_{i=1}^2 \{x_{1i}, \dots, x_{ni} \in \mathbf{Z}/n_i\mathbf{Z} \ : \ f_1(x_{1i}, \dots, x_{ni}) \equiv\equiv \cdots \equiv f_r(x_{1i}, \dots, x_{ni}) \equiv 0 \pmod{n_i}\}$$

sont en bijection à travers l'isomorphisme chinois sur chaque composante. On a clairement que via le théorème chinois, un élément $x_1, \dots, x_n \in \mathbf{Z}/n_1n_2\mathbf{Z}$ tel que $f_\ell(x_1, \dots, x_n) \equiv \pmod{n_1n_2}$ donne lieu en réduisant modulo n_1 et n_2 à un élément de $\mathbf{Z}/n_i\mathbf{Z}$ tel que $f_\ell(x_1, \dots, x_n) \equiv 0 \pmod{n_i}$. Réciproquement, on se donne $x_{1i}, \dots, x_{ni} \in \mathbf{Z}/n_i\mathbf{Z}$ tels que $f_\ell(x_{1i}, \dots, x_{ni}) \equiv 0 \pmod{n_i}$. On sait alors qu'il existe via φ un unique $x_i \in \mathbf{Z}n_1n_2\mathbf{Z}$ tel que $x_i \equiv x_{1i} \pmod{n_i}$. Mais alors

$$f_\ell(x_1, \dots, x_n) \equiv f_\ell(x_{1i}, \dots, x_{ni}) \equiv 0 \pmod{n_i}.$$

Ainsi, $n_1, n_2 \mid f_\ell(x_1, \dots, x_n)$ et n_1 et n_2 sont premiers entre eux donc $n_1n_2 \mid f_\ell(x_1, \dots, x_n)$ et $f_\ell(x_1, \dots, x_n) \equiv 0 \pmod{n_1n_2}$. On a donc bien le résultat. De proche en proche, si $N = \prod_{i=1}^r p_i^{\alpha_i}$, on a une bijection entre

$$\{x_1, \dots, x_n \in \mathbf{Z}/N\mathbf{Z} \ : \ f_1(x_1, \dots, x_n) \equiv \cdots \equiv f_r(x_1, \dots, x_n) \equiv 0 \pmod{N}\}$$

et

$$\prod_{i=1}^r \{x_{1i}, \dots, x_{ni} \in \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z} \ : \ f_1(x_{1i}, \dots, x_{ni}) \equiv \cdots \equiv f_r(x_{1i}, \dots, x_{ni}) \equiv 0 \pmod{p_i^{\alpha_i}}\}.$$

Ici, on pouvait raisonner en utilisant des opérations du pivot de Gauß. Soit $(x, y) \in (\mathbf{Z}/18\mathbf{Z})$ une solution du système. On a alors en effectuant $L_1 \leftarrow 3L_1 - 2L_2$, le système

$$\begin{cases} y = -1 \\ 3x + 4y = 2 \end{cases}$$

Noter qu'ici on ne travaille pas sur un corps et 3 n'est pas inversible dans $\mathbf{Z}/18\mathbf{Z}$, si bien que le système obtenu n'est pas équivalent[4] au système initial ! On obtient alors grâce à la seconde équation que $3x = 6$ soit comme précédemment $x = 2, 8, 14$ modulo 18. Mais, si $y = -1$, la première équation du système fournit $2x = 4$, ce qui implique $x = 2, 11$ modulo 18. Finalement, on constate qu'il existe une unique solution $(x, y) = (2, -1)$.
Une autre méthode consiste à écrire $18 = 3^2 \times 2$ et utiliser le remarque précédente. On résoud d'abord dans $\mathbf{Z}/2\mathbf{Z}$ (qui est un corps). Modulo 2, le système devient

$$\begin{cases} y = 1 \\ x = 0. \end{cases}$$

Par ailleurs, on résoud dans $\mathbf{Z}/9\mathbf{Z}$ (qui n'est pas un corps). Modulo 9, le système devient

$$\begin{cases} 2x + 3y = 1 \\ 3x + 4y = 2. \end{cases}$$

Ici, 2 est inversible modulo 9 d'inverse 5 et la première équation équivaut à $x = 5 - 15y = 5 + 3y$. On peut alors réinjecter dans la seconde équation et obtenir $4y = 2 - 15 = 5$ et de même, 4 est inversible modulo 9 d'inverse 7 et $y = 35 = -1$ modulo 9. On obtient donc $x = 2$ et ce couple est bien l'unique solution. Finalement, l'isomorphisme chinois fournit une unique solution à travers φ^{-1} qui est donné par $\varphi^{-1}(\overline{x}^2, \overline{y}^9) = \overline{-9x + 10y}^{18}$. On a donc que notre unique solution est $(\overline{-9 \times 0 + 10 \times 2}^{18}, \overline{-9 \times 1 - 10 \times 1}^{18} = (2, -1)$. On retrouve bien le même résultat !

4. On procède ici comme d'habitude en essayant de mettre sous forme canonique. On remarque que 13 est premier donc $\mathbf{Z}/13\mathbf{Z}$ est un corps. On a alors pour écrire un début d'identité remarquable, d'inverser 2 modulo 14, ce qui est possible et son inverse vaut 7. Ainsi

$$x^2 + x + 7 = (x + 7)^2 - 42 = (x + 7)^2 - 3.$$

On cherche donc si 3 est un carré modulo 13. Or, on remarque que $4^2 = 3$ modulo 13 et donc comme on travaille sur un corps, on a que deux racines carrées de 3, qui sont 4 et -4. On a alors que les solutions de $x^2 + x + 7 = 0$ modulo 13 sont données par $4 - 7 = -3 = 10$ et $-4 - 7 = -11 = 2$ modulo 13.
On peut procéder de même à la différence qu'ici on en travaille plus sur un corps. L'équation est équivalente à $(x - 2)^2 = 1$ modulo 12, soit $(x - 2 - 1)(x - 2 + 1) \equiv 0 \,(\mathrm{mod}\, 12)$ mais attention qu'on n'a pas intégrité de $\mathbf{Z}/12\mathbf{Z}$. On peut alors lister les carrés de $\mathbf{Z}/12\mathbf{Z}$ et constater que les solutions de $t^2 \equiv 1 \,(\mathrm{mod}\, 12)$ sont $-5, -1, 1, 5$. L'ensemble des solutions est donc $1, 3, 7, 9$. Noter qu'on a plus de solutions que le degré.
On pouvait aussi utiliser la remarque de la question précédente et résoudre modulo 3 et modulo 4. Modulo 3, on a un corps et l'équation devient $x^2 - x = 0$ qui a deux solutions 0 et 1. Modulo 4, on obtient $x^2 = 1$ qui a pour solutions -1 et 1. On écrit alors notre isomorphisme chinois $\varphi^{-1}(\overline{x}^3, \overline{y}^4) = \overline{-8x + 9y}^{12}$ de sorte qu'on obtient bien 4 solutions qui sont

$$\overline{-8 \times 0 + 9 \times 1}^{12} = 9, \quad \overline{-8 \times 0 - 9 \times 1}^{12} = 3, \quad \overline{-8 \times 1 + 9 \times 1}^{12} = 1, \overline{-8 \times 1 - 9 \times 1}^{12} = 7.$$

On retombe bien à nouveau sur les mêmes solutions ! Ouf !

Exercice 7. 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.

4. Cela revient à multiplier à gauche la matrice du système par la matrice $\begin{pmatrix} 3 & -2 \\ 0 & 1 \end{pmatrix}$ qui est non inversible modulo 18.

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

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

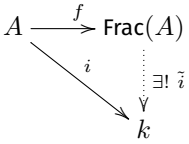
   De même $\frac{ab}{st} = \frac{a'b'}{s't'}$, car

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

   Les deux opérations sont donc bien définies. Montrons maintenant que $(S^{-1}A, +, .)$ est un anneau commutatif : soient $\frac{a}{s}$, $\frac{b}{t}$, $\frac{c}{u} \in S^{-1}A$,
   - $+$ 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 $a, b \in A$, $f(a + b) = \frac{a+b}{1} = \frac{a \cdot 1 + b \cdot 1}{1} = f(a) + f(b)$;
   - $f(1) = \frac{1}{1}$.

   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 $S^{-1}A$; 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 $\frac{a}{s} \cdot \frac{s}{a} = \frac{1}{1}$ 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[5] $\tilde{i}$: Frac$(A) \to k$ injectif tel que $\tilde{i} \circ f = i$, autrement dit tel que le diagramme suivant commute.



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

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[6] 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 $A_P/S^{-1}P$ un corps, appelé *corps résiduel*. Par propriété universelle du corps de fraction, on obtient un morphisme injectif $\mathrm{Frac}(A/P) \to A_P/S^{-1}P$ donné par[7] $\frac{\pi(a)}{\pi(s)} \to \pi_P\left(\frac{a}{s}\right)$ 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 $\pi : A \to A/P$ 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 !).

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 $\sqrt{P} = P$. En déduire que $\sqrt{I}$ est inclus dans l'intersection des idéaux premiers de A qui contiennent I.

3. Soient $a \notin \sqrt{I}$ et $\mathcal{E}$ la collection de tous les idéaux de A contenant I mais aucune puissance de a. Établir que $\mathcal{E}$ possède un élément maximal qui est un idéal premier de A. En déduire que $\sqrt{I}$ est égale à l'intersection des idéaux premiers de A qui contiennent I.

4. 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.

Solution.

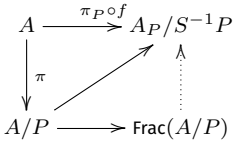
1. Soient $x, y \in \sqrt{I}$. On a alors deux entiers naturels n et m tels que $x^n, y^m \in I$. Ainsi, puisque l'anneau est commutatif,

$$(x-y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} (-1)^{n+m-k} x^k y^{n+m-k}.$$

Si $k \geqslant n$, $x^k = x^n x^{k-n} \in I$ donc $\binom{n+m}{k}(-1)^{n+m-k}x^k y^{n+m-k} \in I$ tandis que si $k < n$, alors $n+m-k \geqslant m$ et $y^{n+m-k} \in I$ de sorte que $\binom{n+m}{k}(-1)^{n+m-k}x^k y^{n+m-k} \in I$. Ainsi, on a bien $(x-y)^{n+m} \in I$ et $x+y \in \sqrt{I}$. Enfin, pour $x \in \sqrt{I}$ tel que $x^n \in I$, comme A est commutatif, pour tout $a \in A$, $(ax)^n = a^n x^n \in I$. On a donc bien que $\sqrt{I}$ est un idéal qui contient clairement I (prendre $n = 1$). On a en particulier $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. Soit alors $x \in \sqrt{\sqrt{I}}$. Il existe n tel que $x^n \in \sqrt{I}$ donc il existe m tel que $(x^n)^m = x^{nm} \in I$ et donc $x \in \sqrt{I}$ ce qui démontre que $\sqrt{I} = \sqrt{\sqrt{I}}$.

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

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



2. Soit $x \in \sqrt{P}$ et $n \geqslant 1$ tel que $x^n = x \cdot x^{n-1} \in P$. 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 $x^{n-1} = x \cdot x^{n-2} \in P$, donc soit $x \in P$ soit $x^{n-2} = x \cdot x^{n-3} \in P$. On continue ainsi jusqu'à obtenir $x \in P$. On a donc $\sqrt{P} = P$.
Soient alors $a \in \sqrt{I}$ et $\mathfrak{P}$ un idéal premier de A contenant I. On a par définition qu'il existe un entier naturel non nul tel que $a^n \in I \subseteq \mathfrak{P}$ de sorte que $a \in \mathfrak{P}$ puisque ce dernier est premier.

3. L'ensemble $\mathcal{E}$ n'est pas vide car il contient I et il est ordonné pour l'inclusion. Il est par ailleurs inductif car pour toute famille $(I_i)_{i\in I}$ totalement ordonnée de $\mathcal{E}$, on voit que $\bigcup_{i\in I} I_i$ est un idéal[8] de A contenant I et aucune puissance de a, donc un majorant de $(I_i)_{i\in I}$ dans $\mathcal{E}$. Par le lemme de Zorn, $\mathcal{E}$ possède un élément maximal P qui est un idéal de A contenant I et aucune puissance de a. Montrons que P est premier. Soient x, y non dans P et montrons que $xy \notin P$. On a que $P + Ax$ est un idéal de A contenant strictement P donc par maximalité, on a donc qu'il contient une puissance de a. De même pour $P + Ay$. Ainsi, il existe k, ℓ deux entiers naturels non nuls tels que $a^k = p + ax$ et $a^\ell = q + by$ avec $p, q \in P$ et $a, b \in A$. On a alors

$$a^{k+\ell} = (p + ax)(q + by) = pq + aqx + bpy + (ab)(xy).$$

On a alors que $pq, aqx, bpy \in P$ car P est un idéal mais par définition P ne contient aucune puissance de a si bien que $a^{k+\ell} \notin P$. On doit donc avoir $xy \notin P$ et on a bien que P est premier contenant I et aucune puissance de a. Il s'ensuit en particulier que $a \notin P$. On a donc que l'intersection des idéaux premiers de A contenant I est inclus dans $\sqrt{I}$ et par conséquent égalité au vu de la question précédente !
On pouvait aussi utiliser la localisation introduite dans l'exercice 7. Soit $x \notin \sqrt{I}$ et $S = \{x^n \ : \ n \in \mathbf{N}\}$. La partie S est multiplicative : si $x^n, x^m \in S$ 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 à $a \in A$ associe 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 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 $x \neq \sqrt{I}$. 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.
Noter qu'on utilise le théorème de Krull qui repose lui aussi sur le lemme de Zorn et l'axiome du choix auquel on n'échappe pas ici !

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

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.

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 $\pi : A \to A/\mathfrak{M}$ 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.

8. La réunion d'idéaux, comme pour les groupes, n'est pas en général un idéal. Ici, on a bien un idéal car la famille est totalement ordonnée. En effet, si $x, y \in \bigcup_{i\in I} I_i$, alors il existe i_x et i_y tels que $x \in I_{i_x}$ et $y \in I_{i_y}$. Comme la famille est totalement ordonnée, on peut supposer que $I_{i_x} \subseteq I_{i_y}$ de sorte que $x, y \in I_{i_y}$ et alors $x+y \in I_{i_y} \subseteq \bigcup_{i\in I} I_i$.

2. Supposons que $x^k = 0$ pour $k \in \mathbf{N}^\times$. On pose alors [9]

$$u = \sum_{n=0}^{+\infty} (ax)^n = \sum_{n=0}^{+\infty} a^n x^n = \sum_{n=0}^{k-1} a^n x^n$$

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 $a \in \mathrm{rad}(A)$. 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

$$\mathrm{rad}(\mathbf{Z}) = \bigcap p \text{ premier} p\mathbf{Z} = \{0\}.$$

De même, les idéaux de $\mathbf{R}[X]$ sont les idéaux engendrés par un polynôme irréductible de $\mathbf{R}[X]$ et $\mathrm{rad}(\mathbf{R}[X]) = \{0\}$. La discussion page 3 fournit que

$$\mathrm{rad}\left(\mathbf{Z}/n\mathbf{Z}\right) = \bigcap_{\substack{p|n \\ p \text{ premier}}} p\mathbf{Z}/n\mathbf{Z} = r(n)\mathbf{Z}/n\mathbf{Z}$$

avec $r(n) = \prod_{p|n} p$ le *radical* [10] de n.

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

Exercice 10. Un anneau commutatif est dit *local* s'il n'admet qu'un seul idéal maximal.

1. Montrer qu'un anneau commutatif 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 qu'un anneau commutatif est local si, et seulement si, pour tout élément x de cet anneau, au moins l'un de x ou $1-x$ est inversible.

3. Un élément x est dit *idempotent* si $x^2 = x$. Montrer que si A est un anneau local, alors ses seuls idempotents sont 1 et 0. Donner un exemple d'anneau pour lequel la réciproque est fausse.

4. Soient k un corps et n un entier strictement positif. Montrer que $k[x]/(x^n)$ est un anneau local, et déterminer son idéal maximal.

5. Soit p un nombre premier, et soit $\mathbf{Z}_{(p)}$ la localisation de $\mathbf{Z}$ par rapport à l'idéal premier (p) (voir l'exercice **3**). Montrer que $\mathbf{Z}_{(p)}$ est local, et calculer son idéal maximal.

Montrer que cet ensemble, muni de la somme et du produit induits par ceux pour les fonctions continues, est un anneau commutatif local.

Solution.

1. Notons $I = \{x \in A \mid x \notin A^\times\}$. Supposons que c'est un idéal. Soit J un idéal de A. Alors pour tout $y \in J$, $y \notin A^\times$ car sinon $J = A$, donc $J \subset I$ et I est alors maximal et c'est le seul car il contient tous les autres idéaux de A qui est donc local.
Réciproquement, supposons A local et montrons que I est un idéal. Soit M l'idéal maximal de A, il est contenu dans I car tous les éléments de M sont non inversibles. Soient $x, y \in I$ et montrons que $x-y \in I$. Comme x et y sont non inversibles, ils sont contenus dans un idéal maximal qui est nécessairement M qui est le seul idéal maximal de A. On a donc que $x-y$ est contenu dans M qui est contenu dans I donc $x-y \in I$. Comme I est non vide car $0 \in I$ on a bien que $(I,+)$ est un sous-groupe de $(A,+)$. En plus, si $x \in I$, on a que l'idéal engendré par x est forcément contenu dans M, donc pour tout $a \in A$, $ax \in M \subset I$.

2. Supposons A local et supposons $x \notin A^\times$; alors $x \in I = A \backslash A^\times$ qui est un idéal. Si $1-X \in I$, alors $1 = 1-x+x \in I$ mais $1 \in A^\times$; donc $1-x \notin I$ et donc $1-x \in A^\times$. De même, si $1-x \notin A^\times$ alors $1-x \in I$ et si $x \in I$ alors $1 \in I$, donc $x \notin I$ et $x \in A^\times$.
Réciproquement, supposons pour tout $x \in A$, $x \in A^\times$ ou $1-x \in A^\times$. Soit M un idéal maximal de A et soit $y \in A \backslash M$ alors $(y, M) = A$ et il existe $a \in A$, $m \in M$ tels que $1 = ay + m$ donc $ay = 1-m \in A^\times$ car $m \in M \neq A$ donc $m \in A^\times$. On a donc montré que (y) contenait un élément inversible, donc $(y) = A$. On a alors que $y \in A^\times$. On a montré que $A \backslash M = A^\times$ donc $A \backslash A^\times = M$ est un idéal et donc A est local.

9. Reconnaître la série $\frac{1}{1-ax}$.

10. Qui intervient notamment dans la célèbre conjecture abc qui explore le lien entre les structures additive et multiplicative des entiers.

3. Soit $x \in A$ tel que $x^2 = x$, alors $x^2 - x = x(x-1) = 0$ et x et $x-1$ sont des diviseurs de zéro. Comme A est local on a que : soit $x \in A \in A^\times$ et dans ce cas $x = 1$, soit $x - 1 \in A^\times$ et dans ce cas $x = 0$.
Si $A = \mathbf{Z}$ alors il est intègre donc si $x^2 = x$ on a que $x = 1$ ou $x = 0$, donc les seuls idempotents sont 1 et 0 mais $\mathbf{Z}$ n'est pas local car pour tout nombre premier p, l'idéal $p\mathbf{Z}$ est maximal.

4. Les idéaux de $k[x]/(x^n)$ sont en bijection avec les idéaux de $k[x]$ qui contiennent (x^n) ; comme $k[x]$ est principal, ils sont engendrés par un $P \in k[x]$ tel que $(x^n) \subseteq (P)$, c'est-à-dire tels que P divise (x^n), ce qui implique que $P = x^k$ avec $k \leqslant n$. Le seul idéal maximal est alors (x) car pour tout $k \leq n-1$, on a

$$(x^n) \subseteq (x^{n-1}) \subseteq \cdots \subseteq (x^k) \subseteq \cdots \subseteq (x)$$

5. Pour rappel, $\mathbf{Z}_{(p)} = S^{-1}\mathbf{Z}$ où $S = A\backslash(p)$ qui est une partie multiplicative de $\mathbf{Z}$. On a déjà montré que l'idéal engendré par l'image de (p) était le seul idéal maximal de $\mathbf{Z}_{(p)}$ (cf. feuille 3 exercice 2, question 7.)

2 Anneaux euclidiens, factoriels, principaux, noethériens

Exercice 11. 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

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

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

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

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 $i \in \{1, \ldots, r\}$, 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. Le pgcd de tous les éléments de I est alors

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

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

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 $a_1, \ldots, a_r$ d'éléments de I. En appliquant **2.** à $a_1/d, \ldots, a_r/d$, 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.

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 $a \in I$, $\text{pgcd}(a, x) \mid x$ donc a moins de facteurs irréductibles que x et est dans I d'après **1.** mais donc par minimalité, $\text{pgcd}(a, x) = ux$ 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.

11. Ce qui est bien défini puisque le nombre de facteurs irréductibles des éléments non nul est une partie non vide de $\mathbf{N}$.

On peut en revanche construire des anneaux de Bézout non principaux comme l'anneau des fonctions holomorphes ou certains anneaux d'entiers.

Exercice 12. 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 11 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 :
$$a = u p_1 \cdots p_r,$$
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, $(p_1)...(p_r) = (a)$ 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 13. Dans l'anneau $A = \mathbf{Z}[i\sqrt{5}]$, trouver deux éléments qui n'ont pas de pgcd et deux éléments qui n'ont pas de ppcm.

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[12] $\overline{u} \in A$ 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[13] $u = \pm 1$ 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[14] $u = u' = 3$ 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[15] $3(2 + i\sqrt{5})$. 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[16] 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

12. Car si $u = a + bi$ avec $a, b \in \mathbf{Z}$, $\overline{u} = a - bi$.
13. On voit facilement que $a^2 + 5b^2 = 1$ équivaut à $a = \pm 1$ et $b = 0$.
14. 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 $\mathbf{C}$.
15. 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 !
16. 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.

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.

Exercice 14. 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 [17].
   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/docs/holomorphe.pdf`. 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 15. 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 [18] 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 $\nu_p(n)$ 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.

17. Car on rappelle qu'un anneau noethérien et intègre possède la propriété d'existence de la décomposition en produit d'irréductibles modulo les inversibles.
18. 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 $b0 \pmod p$ 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 $a^20 \pmod p$ car $b^20 \pmod p$ et $a^2 \equiv -b^2 \pmod p$. Si on pose $x = ab^{-1}$ on a alors que $x0 \pmod p$ 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 $a0 \pmod p$ 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 $p3 \pmod 4$. 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 [19] 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

$$-1 \text{ est un carré dans } \mathbf{F}_p \quad \Longleftrightarrow \quad p3 \pmod 4 .$$

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 [20] $X^{\frac{p-1}{2}} - 1$. 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 $A = \mathbf{Z}[i] \cong \mathbf{Z}[X]/(X^2+1)$. On utilise alors le fait que pour deux idéaux I et J de A, alors

$$(A/I)/J = (A/I)/\pi(J)$$

avec $\pi = A \to A/I$ la surjection canonique et où $\pi(J)$ est un idéal car π est surjective. On sait alors par le cours que $\pi(J) = (I+J)/I$ et le troisième théorème d'isomorphisme fournit

$$(A/I)/J = (A/I)/\pi(J) = (A/I)/((I+J)/I) \cong A/(I+J).$$

Par symétrie, il vient

$$(A/I)/J \cong (A/J)/I \cong A/(I+J)$$

19. 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 $(p-1)! \equiv 1 \times (-1) \equiv -1 \pmod p$.

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

et on peut en fait faire "commuter les quotients"! Ainsi, dans notre cas,

$$A/(p) \cong \left(\mathbf{Z}[X]/(X^2+1)\right)/(p) \cong \mathbf{Z}[X]/(p, X^2+1) \cong (\mathbf{Z}[X]/(p))/(X^2+1).$$

Or, à partir du fait que[21] $\mathbf{Z}[X]/(p) \cong \mathbf{F}_p[X]$, on a $(\mathbf{Z}[X]/(p))/(X^2+1) \cong \mathbf{F}_p[X]/(X^2+1)$ si bien qu'on a

$$A/(p) \cong \mathbf{F}_p[X]/(X^2+1).$$

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. On a en réalité que si k est un corps et que $P \in k[X]$ non nul, alors $k[X]/(P)$ est intègre si, et seulement si, $k[X]/(P)$ est un corps si, et seulement si, P est irréductible. On peut le voir en construisant un inverse à l'aide du théorème de Bézout comme dans le TD ou en disant que $k[X]$ est principal car k est un corps donc P irréductible équivaut à (P) premier non nul (qui équivaut donc à $k[X]/(P)$ intègre) qui équivaut à (P) maximal (qui équivaut à $k[X]/(P)$ corps). Enfin, si le degré de P est inférieur à 3, être irréductible sur k équivaut à ne pas avoir de racine sur k. Le résultat tombe en défaut pour des degrés supérieurs[22] mais on a un critère le généralisant que vous trouverez dans le chapitre 3 du Perrin! Je rappelle enfin que les irréductibles de $\mathbf{C}[X]$ sont les polynômes de degré 1 et ceux de $\mathbf{R}[X]$ les polynômes de degré 1 ou les polynômes de degré 2 sans racines réelles[23] comme on l'a établi en TD! En revanche, on verra que sur $\mathbf{Q}$ ou un corps fini, il existe des polynômes irréductibles de tout degré!

Exercice 16. 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 ν 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 $b \in B^\times \cup \{0\}$ tel que $b - a \in (x)$, *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[24] $x \in B \backslash (B^\times \cup \{0\})$ tel que $\nu(x)$ 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 $\nu(b) < \nu(x)$. Si $b = 0$ on a que $a \in (x)$ et donc $\pi(0) = \pi(a)$. Sinon, $\nu(b) < \nu(x)$ 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[25] $\alpha = \frac{1+i\sqrt{19}}{2}$ 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[26] $\mathbf{Z}$. 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

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

21. En effet, la réduction modulo p des coefficients fournit un morphisme surjectif $\mathbf{Z}[X] \to \mathbf{F}_p[X]$ de noyau (p).
22. Comme par exemple, $(X^2+1)^2$ sur $\mathbf{R}[X]$.
23. Car si P est de degré au moins 3, il possède une racine complexe z. Si $z \in \mathbf{R}$, P n'est pas irréductible et si $z \in \mathbf{C} \smallsetminus \mathbf{R}$, alors $\overline{z}$ est aussi racine de P et P est divisible par $(X-z)(X-\overline{z}) \in \mathbf{R}[X]$ n'est pas irréductible non plus!
24. Bien noter que puisque B n'est pas un corps, $B\backslash(B^\times \cup \{0\}) \neq \varnothing$.
25. 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 $(X-\alpha)(X-\overline{\alpha})$.
26. C'est un résultat très important. Voir par exemple le lemme 3.31 du Perrin.

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 $\tilde{\varphi}(aX + b) = \tilde{\varphi}(a'X + b')$ 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 $b = \pm 1$ donc $z = \pm 1$. 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 $\beta^2 - \beta + 1 = 1 \neq 0$ 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[27] : pour tout $a+(x) \in A/(x)$ il existe b inversible ou $b = 0$ tel que $a+(x) = b+(x)$. Si $b = 0$ alors $a+(x)$ 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.

► **Remarque.–** Cela découle qu'un corps de cardinal p est de caractéristique p et contient $\mathbf{F}_p$ comme sous-corps premier donc lui est égal. On peut le redémontrer en considérant le morphisme si k est un corps de cardinal p

$$f : \left\{ \begin{array}{ccc} \mathbf{Z} & \longrightarrow & k \\ n & \longmapsto & n \cdot 1_k. \end{array} \right.$$

Ce morphisme a pour noyau un idéal de $\mathbf{Z}$ de la forme $c\mathbf{Z}$ tel que $\mathbf{Z}/c\mathbf{Z}$ soit un sous-anneau de k intègre. Cela impose c premier et par cardinalité, $c = p$ de sorte que le théorème de factorisation fournit $k \cong \mathbf{Z}/p\mathbf{Z}$. On pouvait aussi raisonner en termes de groupe sous-jacent et voir qu'un isomorphisme de groupes avec $\mathbf{Z}/2\mathbf{Z}$ ou $\mathbf{Z}/2\mathbf{Z}$ s'étendait naturellement en un isomorphisme d'anneaux (et même de corps).

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 $u, v \in \mathbf{Q}$. ($x = \frac{a\bar{b}}{b\bar{b}} = \frac{1}{N(b)}(a\bar{b}) \in \mathbf{Q}[\alpha]$). Soit n la partie entière de v. Alors $v \in [n, n+1[$. Supposons[28] $v \notin \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$ et soient s, t les entiers les plus proches de u et de v respectivement. Alors $|s - u| \leqslant \frac{1}{2}$, $|t - v| \leqslant \frac{1}{3}$. On pose $q = s + t\alpha$ et donc $q \in A = \mathbf{Z}[\alpha]$. On a alors que $N(x-q) = N((u-s)+(v-t)\alpha) = (s-u)^2+(s-u)(t-v)+5(t-v)^2 \leq \frac{1}{4}+\frac{1}{6}+\frac{5}{9} = \frac{35}{36} < 1$. On pose $r = a - bq \in A$. On a alors que $a = bq + r$ et $N(r) < N(b)$.
Supposons maintenant $v \in \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$. On prend $2x = 2u + 2v\alpha$ et $2v \in \left]2n + \frac{2}{3}, 2n + 1 + \frac{1}{3}\right[$, si m est la partie entière de $2v$ alors $2v \notin \left]m + \frac{1}{3}, m + \frac{2}{3}\right[$. 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 $a \in I$, $a \neq 0$ tel que $N(a)$ soit minimal parmi les éléments non nuls de I. Montrons que $I = (a)$. Soit $x \in I$. 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 $x \in (a)$, donc $I \subseteq (a)$ et $I = (a)$.
Sinon $2x = aq + r$, $N(r) < N(a)$ 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 $x \in (a)$ et à nouveau $I = (a)$. On peut donc supposer que $a \in (2)$ et on peut même 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.

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

Exercice 17. On rappelle qu'un anneau commutatif A est *noethérien* si, pour toute chaîne d'idéaux

$$I_0 \subset I_1 \subset I_2 \subset \dots$$

de A, il existe un entier N tel que si $n \geq N$, alors $I_n = I_{n+1}$.
Montrer que l'anneau $C^0([0,1])$ des fonctions continues $[0,1] \to \mathbf{R}$ n'est pas noethérien. Pour ce faire, on montrera que l'idéal des fonctions s'annulant en 0 n'est pas finiment engendré.

Solution. On peut montrer plus généralement que l'anneau $A = \mathcal{C}^0(X)$ des fonctions continues sur un espace métrique compact X est noethérien si, et seulement si, X est fini. En effet, soit $x_0 \in X$. Supposons que $\{x_0\}$ n'est pas ouvert et pour $n \geqslant 1$, soit $f_n : x \in X \to d(x, x_0)^{\frac{1}{n!}}$ où d désigne la distance dans[29] X. Si on pose I_n l'idéal engendré par f_n dans A, alors la suite $(I_n)_{n\in\mathbf{N}}$ est une suite croissante[30] d'idéaux de A qui ne stationne pas[31]. Donc $\{x_0\}$ est forcément ouvert et X est discret. A est donc isomorphe à $\mathbf{R}^X$, les applications de X dans $\mathbf{R}$ qui est noethérien si X est fini.
Réciproquement, si X est fini alors $A = \mathcal{C}^0(X)$ est isomorphe à $\mathbf{R}^X$ qui est noethérien.

Exercice 18. On considère le nombre complexe $\zeta := e^{2\pi i/3}$ et l'on définit un sous-groupe additif de $\mathbf{C}$ en posant $R := \mathbf{Z} + \mathbf{Z}\zeta$.

1. Montrer que R est un sous-anneau de $\mathbf{C}$, puis que R est isomorphe, en tant qu'anneau, à $\mathbf{Z}[X]/(X^2 + X + 1)$.
2. Établir la majoration :
$$\sup_{z\in\mathbf{C}} \inf_{\alpha\in R} |z - \alpha| < 1.$$
Indication : Il est recommandé de tracer une figure.
3. Montrer que R est un anneau euclidien.
Quel est le groupe mutiplicatif $R^\times$ des unités de R ?
4. Dans la suite de cette partie, on désigne par p un nombre premier et l'on note $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$.
Montrer qu'il existe des isomorphismes d'anneaux
$$R/pR \cong \mathbf{Z}[X]/(p, X^2 + X + 1) \cong \mathbf{F}_p[X]/(X^2 + X + 1).$$
5. Montrer que, si $p \neq 3$, les conditions suivantes sont équivalentes :
   (a) Le polynôme $X^2 + X + 1$ admet un racine dans $\mathbf{F}_p$;
   (b) Le polynôme $X^3 - 1$ admet une racine $\neq 1$ dans $\mathbf{F}_p^\times$;
   (c) $p \equiv 1 \pmod 3$.
6. Montrer que, si $p \neq 3$, les conditions suivantes sont équivalentes :
   (a) $p \equiv 1 \pmod 3$;
   (b) p n'est pas premier dans R ;
   (c) Il existe (x, y) dans $\mathbf{Z}^2$ tel que $p = x^2 - xy + y^2$.
7. Dans R, l'élément 3 est-il premier ?

Solution.

1. C'est assez clair que R est un sous-anneau de $\mathbf{C}$. On remarque que ζ est racine du polynôme $P(X) = X^2 + X + 1$. Si $\phi : \mathbf{Z}[X] \to \mathbf{C}$ est le morphisme d'anneau défini par : $\phi(X) = \zeta$, il se factorise par l'idéal engendré par P dans $\mathbf{Z}[X]$ et $\mathbf{Z}[X]/(P)$ est isomorphe à l'image de ϕ. L'image de ϕ est le sous-anneau de $\mathbf{C}$ engendré par ζ ; comme ζ vérifie $\zeta^2 = -\zeta - 1$, tout élément de R est combinaison linéaire dans $\mathbf{Z}$ de 1 et ζ, on montre facilement que l'image est égale à R. Et R est isomorphe, en tant qu'anneau, à $\mathbf{Z}[X]/(X^2+X+1)$.
2. Voir le corrigé du DM I, question **6.** de l'exercice 3 dans la démonstration que l'anneau est euclidien. En dessinant R dans $\mathbf{C}$, on montre que tout nombre complexe z est à une distance strictement inférieure à $\frac{\sqrt{3}}{3}$ donc < 1. Et donc $\sup_{z\in\mathbf{C}} \inf_{\alpha\in R} |z - \alpha| < 1$.

29. On a en effet, pour tous $x, y \in X$, que
$$|d(x, x_0) - d(y, x_0)| \leqslant d(x, y)$$
ce qui établit que f_n est continue sur X. On peut aussi raisonner en remarquant que l'image réciproque d'un ouvert est ouverte.

30. Car pour tout $n \in \mathbf{N}$, $f_n = (f_{n+1})^{n+1}$.

31. C'est ici que l'hypothèse $\{x_0\}$ non ouvert intervient. En effet, sinon $f_{n+1} \in I_n$ et il existerait une fonction continue f telle que $f_{n+1} = ff_n$ soit $f_n = f^{n+1}f_n^{n+1}$. On en déduit pour tout $x \neq x_0$ que $f^{n+1} = \frac{1}{f_n^n}$. Mais le fait que $\{x_0\}$ ne soit pas ouvert implique qu'il existe une suite $(y_k) \in X^{\mathbf{N}}$ telle que $\lim_{k\to+\infty} d(x_0, y_k) = 0$. On a donc une contradiction puisque f^{n+1} est continue en x_0 et $\lim_{k\to+\infty} |f|^{n+1} = +\infty$. Noter que dans le cas où $\{x_0\}$ est ouvert, la fonction f définie pour tout $x \neq x_0$ par $x \mapsto \frac{1}{d(x_0,x)}$ et $f(x_)) = 0$ est continue sur X. C'est clair sur $X \setminus \{x_0\}$ et comme il existe $r_0 > 0$ tel que $d(x_0, x) < r_0 \Rightarrow x = x_0$ par caractère ouvert,
$$\forall \varepsilon > 0, \quad \exists r_0 > 0 \quad \text{tel que} d(x_0, x) < r_0 \Rightarrow |f(x) - f(x_0)| = 0 < \varepsilon.$$

3. Voir le corrigé du DM I, question **6.** de l'exercice 3. On montre alors facilement que R est un anneau euclidien pour le stathme défini par

$$N(a+\zeta b) = (a+\zeta b)(\overline{a+\zeta b}) = a^2 - ab + b^2$$

où pour $z \in \mathbf{C}$ on note $\overline{z}$ le conjugué complexe de z. Si $x = a+\zeta b$ et $y = c+\zeta d$ sont deux éléments non nuls de R, considérons $z = \frac{a+\zeta b}{c+\zeta d}$ qui est un élément de $\mathbf{C}$. Si $z = \alpha \in R$, alors $x = y\alpha + r$, avec $r = 0$. Sinon, soit $\alpha \in R$ tel que $|z-\alpha| < 1$ (qui existe d'après la question précédente). On pose alors $r = x - y\alpha$ qui est un élément de R vérifiant $|\frac{r}{y}| = |\frac{x}{y} - \alpha| < 1$; ceci implique que $|r| < |y|$ et donc $N(r) < N(y)$. On a donc bien $x = y\alpha + r$, $\alpha \in R$, $N(r) < N(y)$ ou $r = 0$.
Le groupe multiplicatif $R^\times$ des unités de R est égale à $\{\pm(1+\zeta), \pm\zeta, \pm 1\}$. On le trouve en montrant que les inversibles de R sont exactement les $\alpha \in R$ tels que $N(\alpha) = 1$.

4. Voir le corrigé du DM I, question **5.** de l'exercice 3. Grâce au cours on sait qu'il existe des isomorphismes d'anneaux

$$R/p.R \cong \mathbf{Z}[X]/(p, X^2+X+1) \cong \mathbf{F}_p[X]/(X^2+X+1)\mathbf{F}_p[X],$$

où l'on a posé :

$$(p, X^2+X+1) := p.\mathbf{Z}[X] + (X^2+X+1)\mathbf{Z}[X].$$

5. Puisque $X^3 - 1 = (X-1)(X^2+X+1)$, il est clair que $(a) \iff (b)$. Supposons alors (b). On a donc un élément $x \in \mathbf{F}_p^\times$ d'ordre 3 donc $3 \mid p-1$ par Lagrange et on a (c). Réciproquement, si $p \equiv 1 \pmod 3$, alors $3 \mid p-1 = \#\mathbf{F}_p^\times$ et par le lemme de Cauchy (ou les théorèmes de Sylow), on a un élément d'ordre 3, autrement dit une racine $\neq 1$ de $X^3 - 1$.

6. D'après **5.**, $p \equiv 1 \pmod 3$ équivaut au fait que X^2+X+1 soit scindé dans $\mathbf{F}_p$, ce qui équivaut au fait que

$$R/(p) \cong \mathbf{F}_p[X]/(X^2+X+1)$$

ne soit pas intègre et donc à ce que p ne soit pas premier dans R. On a donc $(a) \iff (b)$. Supposons alors (b), par factorialité et le fait que p ne soit pas irréductible, il existe z, z' des éléments de R qui ne sont pas des unités tels que $p = zz'$ si bien que $p^2 = N(Z)N(z')$ et le fait que z et z' ne soient pas des unités équivaut au fait que $N(Z), N(z') \notin \{\pm 1\}$ de sorte que $N(Z) = N(z') = p$. Écrivant $z = x + \xi y$ avec $x, y \in \mathbf{Z}$, il vient que $p = x^2 - xy + y^2$. Réciproquement, (c) fournit que $p = N(z)$ avec $z = x + \xi y$ et ainsi $p = z\overline{z}$ avec $N(z) = N(\overline{z}) = p \notin \{\pm 1\}$ de sorte que z et $\overline{z}$ ne sont pas des unités. Cela fournit que p n'est pas premier et donc (b), ce qui conclut la preuve.

7. On applique **4.** pour obtenir que $R/(3) \cong \mathbf{F}_3[X]/(X^2+X+1)$ et modulo 3, on a X^2+X+1 qui est réductible (car $X^2+X+1 = (X-1)^2$) si bien que $R/(3)$ n'est pas intègre et (3) n'est pas premier !

3 Anneaux de polynômes

Exercice 19 — Deux résultats très utiles.

1. Soit A un anneau et soit $P \in A[X]$ non nul de coefficient dominant inversible. Pour tout $F \in A[X]$, montrer qu'il existe $Q, R \in A[X]$ tels que $F = PQ + R$ avec $\deg(R) < \deg(P)$ ou $R = 0$.

2. Soit k un corps et P un polynôme irréductible de $k[X]$. Montrer que $k[X]/(P)$ est un corps.

Solution.

1. Soit $F \in A[X]$ et $P \in A[X]$ de coefficient dominant inversible dans A. On cherche à montrer qu'il existe $Q, R \in A[X]$ avec $\deg(R) < \deg(P)$ ou $R = 0$. Autrement dit, si l'on considère $A[X]/(P)$ et la projection canonique $\pi : A[X] \to A[X]/(P)$, on cherche à montrer qu'il existe R avec $\deg(R) < \deg(P)$ ou $R = 0$ tel que $\pi(F) = \pi(R)$. Or, modulo P, on a

$$\pi(P) = a_n\pi(X)^n + \cdots + a_0 \quad \text{si} \quad P = \sum_{i=0}^{n} a_i X^i.$$

Comme a_n est inversible, on obtient que

$$\pi(X)^n = -a_n^{-1}\left(a_{n-1}\pi(X)^{n-1} + \cdots + a_0\right)$$

est une combinaison linéaire à coefficients dans A de $1, \pi(X), \ldots, \pi(X)^{n-1}$. Par récurrence immédiate, on obtient que $\pi(X^k)$ avec $k \geqslant n$ est combinaison linéaire à coefficients dans A de $1, \pi(X), \ldots, \pi(X)^{n-1}$ de sorte qu'il existe $\lambda_0, \ldots, \lambda_{n-1} \in A$ vérifiant

$$\pi(F) = \sum_{i=0}^{n-1} \lambda_i \pi(X)^i = \pi\left(\sum_{i=0}^{n-1} \lambda_i X^i\right).$$

En posant, $R = \sum_{i=0}^{n-1} \lambda_i X^i$, on a $\pi(F) = \pi(R)$ de sorte que $\pi(F-R) = 0$ et il existe $Q \in A[X]$ tel que $F = PQ + R$, ce qu'il fallait démontrer !
Bien noter qu'on perd *a priori* l'unicité du quotient et du reste. Se souvenir que l'onb peut ainsi effectuer une division euclidienne même lorsque l'anneau n'est pas euclidien (comme dans le cas de $\mathbf{Z}[X]$ ou $k[X,Y]$) lorsque le coefficient dominant du polynôme par lequel on divise est inversible !

2. Soit k un corps et P un polynôme irréductible de $k[X]$. Comme $k[X]$ est euclidien (et donc principal et factoriel), on en déduit que (P) est premier non nul et par l'exercice 4 qu'il est donc maximal. Ainsi, $k[X]/(P)$ est un corps.
Une autre façon de voir que $k[X]/(P)$ est un corps est (pusiqu'il est intègre car (P) est premier) de montrer que tout élément non nul admet un inverse. Soit $\pi : k[X] \to k[X]/(P)$ la surjection canonique. Soit $\pi(Q)$ avec $Q \in k[X]$ un élément de $k[X]/(P)$ non nul, autrement dit tel que Q ne soit pas divisible par P. On a alors, puisque P est irréductible que Q et P sont premiers entre eux car $\text{pgcd}(P,Q) \in \{1, P\}$ modulo les constantes non nulles. Comme $k[X]$ est principal, on dispose donc d'une relation de Bézout [32] et donc de $U, V \in k[X]$ tels que $PU + QV = 1$. On a donc, puisque π est un mrophisme d'anneaux, $\pi(Q)\pi(U) = 1$ et donc $\pi(Q)$ est inversible d'inverse $\pi(U)$. Cela fournit en particulier un algorithme pour calculer l'inverse !

Exercice 20.

1. Calculer $A[X]^\times$ lorsque A est un anneau quelconque.

2. Soit B un anneau et A un sous-anneau de B. Soit $b \in B$. On dit que b est *entier* sur A s'il vérifie une équation unitaire :

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0 \quad \text{avec} \quad a_0, \ldots, a_{n-1} \in A.$$

Un anneau intègre est dit *intégralement clos* si pour tout $x \in K = \text{Frac}(A)$, si x est entier sur A alors $x \in A$.

(a) Montrer qu'un anneau factoriel est intégralement clos.

(b) Soit $d \in \mathbf{Z}$ un entier sans facteur carré non nul. On pose :

$$\mathbf{Z}\big[\sqrt{d}\big] = \{a + b\sqrt{d} \in \mathbf{C} \mid a, b \in \mathbf{Z}\}.$$

Montrer que si $d \equiv 1 \pmod 4$, alors $\mathbf{Z}[\sqrt{d}]$ n'est pas intégralement clos.
Indication : Considérer l'élément $\frac{1+\sqrt{d}}{2}$.

Solution.

1. On peut montrer que $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]^\times$ si et seulement si $a_0 \in A^\times$ et $a_1, \ldots, a_n$ sont nilpotents.

2. Soit $x \in K = \text{Frac}(A)$ un élément entier sur A. Comme A est factoriel il existe $p, q \in A$ premier entre eux tels que $x = \frac{p}{q}$; x étant entier sur A il existe $a_0, \ldots, a_{n-1} \in A$ tels que

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0$$

donc $p^n = -a_{n-1}p^{n-1}q - \cdots - a_1pq^{n-1} - a_0q^n$, comme q divise le membre de droite on a que q divise p^n, or on a supposé que p et q étaient premiers entre eux et comme A est factoriel par le lemme de Gauß, on a que q divise 1 et donc q est inversible dans A. On a alors que $x = pq^{-1} \in A$.

3. Considérons $\alpha = \frac{1+\sqrt{d}}{2}$. Alors $\alpha^2 - \alpha - \frac{d-1}{4} = 0$. Comme $d \equiv 1[4]$, on a que α est bien entier donc $\mathbf{Z}[\sqrt{d}]$ n'est pas intégralement clos.

Exercice 21. Montrer qu'un polynôme $P(X,Y) \in \mathbf{Z}[X,Y]$ est tel que $P\big(t^2, t^3\big) = 0$ pour tout $t \in \mathbf{Z}$ si, et seulement si, il existe un polynôme $Q(X,Y) \in \mathbf{Z}[X,Y]$ tel que $P(X,Y) = (X^3 - Y^2) \cdot Q(X,Y)$. En déduire un isomorphisme de $\mathbf{Z}$-algèbres

$$\mathbf{Z}[X,Y]/\big(X^3 - Y^2\big) \cong \{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\} \cong \mathbf{Z}[T^2, T^3].$$

Solution. Commençons par préciser que l'on peut toujours effectuer une division euclidienne dans $k[X]$ pour k corps avec unicité du quotient et du reste. On a vu dans l'exercice 10 du TD III que l'on peut toujours effectuer une division euclidienne (en perdant l'unicité cependant) de P par Q dans $A[X]$ à condition que le coefficient dominant de Q soit inversible [33] dans A. Si jamais le coefficient dominant de Q n'est pas inversible, alors on peut parfois s'en sortir en voyant $A[X] \subseteq \text{Frac}(A)[X]$ et effectuer le division euclidienne dans $\text{Frac}(A)[X]$. Par exemple, soient $P, Q \in A[X,Y] = A[X][Y]$. Si le coefficient dominant de Q vu dans $A[X][Y]$ n'est pas dans $A[X]^\times = A^\times$, alors on effectue la division dans $A(X)[Y]$, ce qui fournit $B, R \in A[X,Y]$ avec $\deg_Y(R) < \deg_Y(Q)$ et $A \in A[X]$ non nul tel que $A(X)P(X,Y) = Q(X,Y)B(X,Y) + R(X,Y)$.

32. Je rappelle (voir l'exercice 11 qu'un anneau factoriel qui vérifie la relation de Bézout est nécessairement principal.

33. Voir le lemme 3.31 du Perrin pour une démonstration.

Venons-en alors à l'exercice à proprement parler. Il est immédiat que si $P \in (X^3 - Y^2)$, alors pour tout entier relatif t, $P(t^2, t^3) = 0$. Réciproquement, supposons que pour tout entier relatif t, $P(t^2, t^3) = 0$. le coefficient dominant de[34] $X^3 - Y^2 \in \mathbf{Z}[X][Y]$ est égal à $-1 \in \mathbf{Z}^\times = \mathbf{Z}[X]^\times$. On peut donc effectuer une division euclidienne de P par $X^3 - Y^2$ si bien qu'il existe $Q, R \in \mathbf{Z}[X, Y]$ avec $\deg_Y(R) < 2$ tels que $P(X, Y) = (X^3 - Y^2)Q(X, Y) + R(X, Y)$. Puisque $\deg_Y(R) < 2$, il existe $A, B \in \mathbf{Z}[X]$ tels que $R(X, Y) = A(X)Y + B(X)$ de sorte que $P(X, Y) = (X^3 - Y^2)Q(X, Y) + A(X)Y + B(X)$. On peut alors évaluer cela en $t \in \mathbf{Z}$ pour obtenir que

$$0 = P(t^2, t^3) = (t^6 - t^6)Q(t^2, t^3) + A(t^2)t^3 + B(t^2) = A(t^2)t^3 + B(t^2).$$

On en déduit (puisque $\mathbf{Z}$ est infini) que $A(X^2)X^3 + B(X^2) = 0$. On voit que $A(X^2)X^3$ ne fait intervenir que des monômes impairs distincts et que $B(X^2)$ ne fait intervenir que des monômes pairs distincts. On en déduit que $A = B = 0$ et donc $R = 0$ et $P \in (X^3 - Y^2)$ et on a bin démontré l'équivalence.
On pose alors $\mathbf{Z}[T^2, T^3] = \{P(T^2, T^3) \ : \ P \in \mathbf{Z}[X, Y]\}$ et on considère le morphisme surjectif de $\mathbf{Z}$-algèbre $f : \mathbf{Z}[X, Y] \to \mathbf{Z}[T^2, T^3]$ définie par $P \mapsto P(T^2, T^3)$. Ce qui précède garantit que le noyau est égal à l'idéal $(X^3 - Y^2)$ si bien qu'au quotient on a bien

$$\mathbf{Z}[X, Y]/\big(X^3 - Y^2\big) \cong \mathbf{Z}[T^2, T^3].$$

Reste donc à voir que $\{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\} \cong \mathbf{Z}[T^2, T^3]$. On a évidemment $\mathbf{Z}[T^2, T^3] \subseteq \{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\}$ puisqu'un tel polynôme n'a pas de terme en T. Réciproquement, si $P \in \{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\}$, alors il existe un $d \in \mathbf{N}$ tel que

$$P = \sum_{\substack{i=0 \\ i \neq 1}}^{d} a_i T^i.$$

Mais pour tout $i \neq 1$, on peut effectuer la division euclidienne de i par 3 pour obtenir l'existence de $q \in \mathbf{Z}$ et $r \in \{0, 1, 2\}$ tel que $i = 3q + r$. Si $r = 0$, alors $T^i = (T^3)^q$ tandis que si $r = 2$, alors $T^i = (T^3)^q T^2$. Enfin, si $r = 1$, on a $i = 3(q - 1) + 4$ et $T^i = (T^3)^{q-1}(T^2)^2$ qui a bien un sens car $q - 1 \geqslant 0$ puisque sinon $q = 0$ et $r = 1$ donc $i = 1$ ce qui est exclu. On a donc bien que $P \in \mathbf{Z}[T^2, T^3]$, ce qui conclut la démonstration. On pouvait aussi traiter les cas i pairs d'un côté et les $i \geqslant 3$ impairs en remarquant que $i - 3$ est positif et pair.

Exercice 22. Soit k un corps et N un entier naturel. On considère l'anneau de polynômes $A := k[X_1, \ldots, X_N]$, un élément $\mathbf{a} = (a_1, \ldots, a_N)$ de k^N et un élément P de A.
Vérifier que l'on définit des idéaux de A en posant

$$I_1 := (P) = P \cdot A \quad \text{et} \quad I_2 := \{Q \in k[X_1, \ldots, X_N] \mid Q(\mathbf{a}) = 0\}.$$

Montrer que I_1 et I_2 sont des idéaux étrangers si, et seulement si, $P(\mathbf{a}) \neq 0$. On rappelle que, par définition, I_1 et I_2 sont des idéaux étrangers de A si $I_1 + I_2 = A$.

Solution. Si I_1 et I_2 sont étrangers, il existe $Q_1 \in I_1$ et $Q_1 \in I_2$ tels que $1 = Q_1 + Q_2$, donc, il existe $Q_1' \in A$ et $Q_2 \in I_2$ tels que $1 = Q_1'(X)P(X) + Q_2(X)$, en particulier, $1 = Q_1(a)P(a) + Q_2(a)$, comme $Q_2(a) = 0$ on a forcément que $P(a) \neq 0$.
Réciproquement, si $P(a) \neq 0$ alors $P(a)$ est inversible et on peut écrire $1 = P(a)^{-1}P + (1 - P(a)^{-1}P)$; on remarque que $P(a)^{-1}P \in I_1$ et $(1 - P(a)^{-1}P) \in I_2$ donc I_1 et I_2 sont étrangers.

Exercice 23. Soit $Q \in \mathbf{Z}[X]$ unitaire. On note $z_1, \ldots, z_n$ ses racines (pas forcément distinctes) dans $\mathbf{C}$. Montrer que

$$\prod_{i \neq j} (z_i - z_j) \in \mathbf{Z}.$$

Solution. On observe que le polynôme en n indéterminées

$$P = \prod_{i \neq j} (X_i - X_j)$$

est un polynôme symétrique de $\mathbf{Z}[X_1, \ldots, X_n]$; en effet, il est clairement invariant pour l'action de toute transposition, et les transpositions engendrent $\mathfrak{S}_n$. D'après le théorème de structure, il existe $R \in \mathbf{Z}[X_1, \ldots, X_n]$ tel que

$$P = R(\sigma_1, \ldots, \sigma_n),$$

où les σ_i sont les polynômes symétriques élémentaires. D'autre part, on a

$$Q = \prod_{i=1}^{n} (z - z_i) = z^n - \sigma_1(z_1, \ldots, z_n)z^{n-1} + \cdots + (-1)^n \sigma_n(z_1, \ldots, z_n),$$

ce qui montre que chaque $\sigma_i(z_1, \ldots, z_n)$ est entier. Du coup,

$$P(z_1, \ldots, z_n) = R(\sigma_1(z_1, \ldots, z_n), \ldots, \sigma_n(z_1, \ldots, z_n))$$

est bien entier comme on voulait.

34. Noter que ce choix est plus judicieux que $A[Y][X]$ car le degré en Y de $X^3 - Y^2$ est strictement inférieur à son degré en X.

Exercice 24.

1. Soit A un anneau factoriel, et soit K le corps des fractions de A. Donner un exemple de polynôme réductible dans $A[X]$ et irréductible dans $K[X]$ et un exemple de polynôme irréductible dans $A[X]$ et réductible dans $K[X]$.
2. Donner les éléments irréductibles de $\mathbf{Z}[X]$ en fonction de ceux de $\mathbf{Q}[X]$ et de $\mathbf{Z}$.
3. Donner une procédure permettant de déterminer si un polynôme de degré au plus 3 est irréductible dans $\mathbf{Z}[X]$.
4. Soit K un corps, et soient $P, Q \in K[X]$ premiers entre eux. Montrer que $P \cdot Y + Q$ est irréductible dans $K[X, Y]$.
5. Soit $a \in \mathbf{Z}$. À quelle condition $X^4 - a$ est-il irréductible dans $\mathbf{Q}[X]$? et $X^4 - aX - 1$ dans $\mathbf{Z}[X]$?

Solution.

1. Si P est un polynôme de $A[X]$ irréductible dans $k[X]$ et $a \in A\backslash\{0\}$ non inversible dans A, alors aP est réductible dans $A[X]$ mais irréductible dans $k[X]$ car $a \in k^\times$. Pour trouver un polynôme irréductible dans $A[X]$ mais réductible dans $k[X]$ il suffit de prendre un polynôme constant irréductible de $A[X]$ qui n'est pas primitif.
2. Un nombre premier $p \in \mathbf{Z}$ est irréductible dans $\mathbf{Z}[X]$ comme polynôme de degré 0. Si P est un polynôme irréductible de $\mathbf{Z}[X]$ de degré $\geqslant 1$, alors forcément son contenu est égal à 1 et donc P est irréductible dans $\mathbf{Q}[X]$ (lemme de Gauß). Inversement si P est irréductible dans $\mathbf{Q}[X]$ alors il existe $n \in \mathbf{Q}$ tel que $nP \in \mathbf{Z}[X]$ et de contenu égal à 1; nP est alors irréductible dans $\mathbf{Z}[X]$.
3. Soit $P(X) = aX^3 + bX^2 + cX + d \in \mathbf{Z}[X]$. D'abord, pour qu'il soit irréductible il faut que $\text{pgcd}(a, b, c, d) = 1$; s'il est réductible dans $\mathbf{Q}[X]$ alors il a une racine (car degré 3) : si $\frac{m}{n} \in \mathbf{Q}$ est une racine de P (avec $(n, m) = 1$) alors n divise a et m divise d. On teste alors tous les diviseurs de a et de d pour trouver la racine éventuelle [35].
4. Le polynôme $PY + Q$ est de contenu égal à 1 dans $K[X][Y]$; il est irréductible dans $K[X][Y]$ si et seulement si il est irréductible dans $K(X)[Y]$. Or le degré de $PY + Q$ en tant que polynôme en Y est égal à 1, il est donc irréductible.
5. Si $P = X^4 - \alpha^2$ alors P est évidemment réductible. C'est en particulier le cas si P a une racine dans [36] $\mathbf{Q}$. Supposons P réductible : il existe alors $b, c, b', c' \in \mathbf{Z}$ tels que $P = (X^2 + bX + c)(X^2 + b'X + c')$ ce qui implique que $b = b'$, $c + c' = b^2$, $b(c - c') = 0$ et $cc' = -a$. Si $b = 0$ alors $c = -c'$ et donc a est un carré ce qui revient au premier cas. Si $c = c'$, $a = -c^2$ (a est négatif), et $2c = b^2$; donc b^2 doit être pair et b est de la forme $b = 2d$. Donc $c^2 = 4d^4$ et $a = -4d^4$. On conclut que P est réductible si et seulement si a est un carré ou a est de la forme $a = -4d^4$.
   Pour $X^4 - aX - 1$, on remarque d'abord que si α est une racine alors α divise 1 donc les seules racines possibles dans $\mathbf{Z}$ sont -1 et 1; on a alors que P a une racine si et seulement si $a = 0$. Si $a \neq 0$, $P = (X^2 + bX + c)(X^2 + b'X + c') = X^4 - aX - 1$ implique $b = b'$, $c' + c = b^2$, $b(c' - c) = -a$ et $cc' = -1$; mais $c, c' \in \mathbf{Z}$ donc on $c + c' = 0$ et $b^2 = 0$ ce qui implique que $a = 0$ et P a une racine, donc est réductible. On a alors P irréductible si et seulement si $a \neq 0$.

Exercice 25. Montrer que les polynômes suivants sont irréductibles.

1. Pour $n > 0$ et p premier, $X^n - p$ sur $\mathbf{Q}$;
2. $X^4 + X + 1$ sur $\mathbf{Q}$;
3. $X^6 + X^2 + 1$ sur $\mathbf{Q}$;
4. Pour $n > 0$, $X^n - T$ sur $K(T)$ (K un corps);
5. $1 + X + \ldots + X^{p-1}$ sur $\mathbf{Q}$, pour p premier.

Solution.

1. On applique le critère d'Eisenstein avec p.
2. On commence par montrer que l'on n'a pas de racine dans $\mathbf{Q}$ car une telle racine $\frac{p}{q}$ vérifierait $q = \pm 1$ et $p = \pm 1$ mais ni 1 ni -1 n'est racine. On raisonne alors par l'absurde et on voit qu'on n'a aucune factorisation du type $(X^2 + aX + b)(X^2 + cX + d)$.
   Une autre preuve est fournie dans le Perrin page 78. On pouvait aussi réduire modulo 2 et vérifier qu'il n'y a pas de racine et que le seul polynôme irréductible de degré 2 unitaire sur $\mathbf{F}_2$ est $X^2 + X + 1$. Ainsi, si $X^4 + X + 1$ n'est pas irréductible, il est égal à
   $$(X^2 + X + 1)^2 = X^4 + X^2 + 1$$
   ce qui est absurde !
3. Plusieurs méthodes sont possibles. Attention que le fait que $X^3 + X + 1$ soit irréductible sur $\mathbf{Q}$ (car sans racine et de degré $\leqslant 3$) implique que $X^6 + X^2 + 1$ est sans racine rationnelle mais pas qu'il est irréductible [37]. On peut alors raisonner par l'absurde et montrer qu'on n'a aucune factorisation du type $(X^2 + aX + b)(X^4 + cX^3 + dX^2 + eX + f)$ (ce qui implique en particulier l'abscence de factorisation comme un produit de trois polynômes de degré 2) ni de la forme $(X^3 + aX^2 + bX + d)(X^3 + eX^2 + fX + g)$ mais c'est un peu fastidieux.

35. Je rappelle qu'un polynôme de degré 2 ou 3 est irréductible sur un corps k si, et seulement s'il n'a pas de racine. La condition nécessaire est évidente et pour la condition suffisante, il suffit de voir qu'un polynôme de degré 2 ou 3 non irréductible s'écrit comme produit de polynômes irréductibles de degré strictement inférieur et que cela fait nécessairement apparaître si $\deg(P) \leqslant 3$ un polynôme irréductible de degré 1 donc une racine !

36. On pouvait ici utiliser la factorisation sur $\mathbf{C}[X]$ et déterminer pour quelles valeurs de a, cela fournissait soit une racine rationnelle soit un produit de deux polynômes de degré 2 à coefficients rationnels.

37. Par exemple, $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$ est réductible mais $X^2 + 4$ est irréductible.

On pouvait sinon raisonner modulo certains nombres premiers. On voit tout de suite que $X^6+X^2+1=(X^3+X+1)^2$ dans $\mathbf{F}_2$ et on vérifie que X^3+X+1 y est irréductible (car de degré 3 sans racine). Ceci nous fournit[38] que X^6+X^2+1 est soit irréductible sur $\mathbf{Q}$ soit est un produit de deux polynômes de degré 3. Mais, on vérifie que dans $\mathbf{F}_3$ on a deux racines (à savoir ± 1) si bien que $X^6+X^2+1=(X-1)(X+1)Q$ avec Q de degré 4 sans racine[39] dans $\mathbf{F}_3$. Cela implique que X^6+X^2+1 est irréductible. En effet, on a vu modulo 2 que soit P est irréductible soit il est produit de deux irréductibles de degré 3. Mais la réduction modulo 3 de P s'écrirait alors comme un produit de deux polynômes de degré 3. La seule possibilité pour obtenir une décomposition de la forme $(X-1)(X+1)Q$ avec Q de degré 4 sans racine est que chaque polynôme de degré 3 se scinde en un polynôme de degré 1 fois un polynôme irréductible de degré 2 et cela impliquerait en particulier que $Q=X^4+X^2+2$ est produit de deux polynômes irréductibles unitaires de degré 2 sur $\mathbf{F}_3[X]$. Mais un polynôme unitaire de degré 2 irréductible sur $\mathbf{F}_3[X]$ est de la forme X^2+aX+b sans racine. Notamment cela impose $b\neq 0$. Testant alors toutes les combinaisons possibles de $a,b\in\mathbf{F}_3$, on constate que les seuls polynômes irréductibles unitaires de degré 2 sur $\mathbf{F}_3[X]$ sont X^2+1, X^2+X-1 et X^2-X-1. On vérifie alors qu'aucun produit de deux de ces polynômes de fournit Q. On en conclut que P n'est pas produit de deux irréductibles de degré 3 et que par conséquent P est irréductible[40].

►**REMARQUE.–** On a notamment que s'il existe p premier tel que $\overline{P}$ soit irréductible modulo p, alors P est irréductible sur $\mathbf{Q}$. Attention en revanche qu'un tel p n'existe pas toujours (on verra notamment que X^4+1 est irréductible sur $\mathbf{Z}$ mais réductible modulo tout premier p. cela a à voir encore une fois avec le groupe de Galois de P (voir par exemple le Théorème 4.13 ici). Vous pourrez trouver des compléments dans le chapitre 4 du cours ou en section III.3 du Perrin.
Terminons par mentionner que factoriser un polynôme sur un corps fini se fait très bien algorithmiquement via l'algorithme de Berlekamp et que cet algorithme et des réductions modulo des nombres premiers bien choisis (grâce aux bornes de Mignotte) permet d'obtenir un algorithme de factorisation sur $\mathbf{Z}$. Rendez-vous lors du cours de calcul formel du semestre prochain si ces thématiques vous intéressent!

4. L'élément T est irréductible dans l'anneau factoriel $K[T]$ et on peut lui appliquer le critère d'Eisenstein (comme en **1.**) qui fournit l'irréductibilité dans $K[T][X]$ et comme le polynôme est primitif, dans $K(T)[X]$.

5. On remarque qu'il s'agit du polynôme cyclotomique[41] Φ_p. On constate que $(X-1)\Phi_p=X^p-1$ et en évaluant en $X+1$, il vient que $X\Phi_p(X+1)=(X+1)^p-1$, autrement dit

$$\Phi_p(X+1)=X^{p-1}+\sum_{k=1}^{p-2}C_{k+1}^p X^k+p.$$

On remarque alors que[42] $p\mid C_{k+1}^p$ pour tout $k\in\{1,\dots,p-2\}$ et on peut alors déduire d'Eisenstein appliqué à p que le polynôme $\Phi_p(X+1)$ est irréductible, ce qui implique que Φ_p est irréductible lui-même[43].

EXERCICE 26.

1. Soient K et L deux corps tels que L contienne K ainsi que $P,Q\in K[X]$. Montrer que le pgcd de P et Q dans $K[X]$ est le même que le pgcd de P et Q dans $L[X]$.
Indication : On pourra commencer par le cas premier entre eux.

38. En effet, $P=X^6+X^2+1$ est primitif et si on écrit sa factorisation en produit d'irréductibles dans l'anneau factoriel $\mathbf{Z}[X]$, alors on obtient des polynômes irréductibles de $\mathbf{Z}[X]$ de degré $\geqslant 1$ donc primitifs et irréductibles sur $\mathbf{Q}[X]$. Par unicité (aux unités près) d'une telle décomposition, on peut donc supposer que la décomposition de P en produit d'irréductibles est de la forme

$$P=\prod_{i=1}^r P_i^{n_i}$$

avec les P_i des polynômes irréductibles de $\mathbf{Z}[X]$ unitaires non constants et 2 à deux non associés. Soit alors p un nombre premier et $\overline{P}$ le polynôme obtenu en réduisant modulo p les coefficients de P. On a (c'est un morphisme d'algèbres) que

$$\overline{P}=\prod_{i=1}^r \overline{P_i}^{n_i}=(X^3+X+1)^2.$$

Puisque les P_i sont unitaires, $\overline{P_i}$ a même degré que P_i. Si on avait un P_i irréductible de degré 2 dans la décomposition de P, alors on obtiendrait un facteur $\overline{P}_i$ de degré 2 qui est soit irréductible soit produit de deux polynômes irréductibles de degré 1, ce qui est exclu car on a un seul facteur irréductible de degré 3 de multiplicité 2. De même, si on avait un P_i de degré 1, alors on aurait une racine modulo p, ce qui n'est pas le cas. Les seuls types de factorisation possibles sont donc P irréductible ou P produit de deux polynômes irréductibles de degré 3.

39. Ici, on obtient le sans racine soit en utilisant que $Q=X^4+X^2+2$ soit en utilisant le fait que sur un corps, x est racine multiple si, et seulement si, $P(x)=P'(x)=0$ (même en caractéristique >0). En effet, si $P=(X-x)^2Q$, il est clair que $P(x)=P'(x)=0$. Réciproquement (noter qu'en revanche la démonstration habituelle à base de formule de Taylor ne fonctionne plus), mais le fait que $P(x)=0$ implique que $P=(X-x)Q$ et donc $P'=(X-x)Q'+Q$ et on voit que $P'(x)=0$ équivaut à $Q(x)=0$ et donc au fait que x soit racine multiple. Attention en revanche que du fait que la dérivée de X^p est nulle en caractéristique p que l'équivalence x est de multiplicité m si, et seulement si, $P(x)=P'(x)=\cdots=P^{(m-1)}(x)=0$ et $P^{(m)}(x)\neq 0$ tombe en défaut! En revanche, on peut établir que cela reste toutefois vrai si $m\leqslant p-1$.

40. On verra que les types de factorisation qui apparaissent modulo p et que l'on a utilisés ici sont liés aux groupes de Galois des polynômes!

41. On reviendra en détails sur ces polynômes importants dans le chapitre sur les corps. Ils sont par exemple à la base d'une démonstration d'une version faible du théorème de la progression arithmétique de Dirichlet stipulant qu'il existe une infinité de nombres premiers $p\equiv 1\pmod n$ pour tout entier naturel n ou du théorème de Wedderburn stipulant que tout corps fini est commutatif.

42. Car pour $k\in\{1,\dots,p-2\}$, $p\mid (k+1)!C_{k+1}^p=p(p-1)\cdots(p-k)$ et $(k+1)!$ est premier à p.

43. Sinon, on a $\Phi_p=Q_1Q_2$ avec Q_1 et Q_2 non constants si bien que $\Phi_p(X+1)=Q_1(X+1)Q_2(X+1)$ avec $Q_1(X+1)$ et $Q_2(X+1)$ non constants, ce qui est absurde.

2. Donner un exemple d'algèbre à division et de polynôme admettant plus de racines que son degré sur cette dernière.

SOLUTION.

1. On a deux anneaux de Bézout. On commence alors par traiter le cas de P et Q premiers entre eux sur L. Il existe alors deux polynômes $U, V \in K[X]$ tels que $PU + QV = 1$. Comme en particulier, $U, V \in L[X]$, on en déduit que P et Q restent premiers entre eux sur K. Réciproquement, si P et Q sont premiers entre eux sur L et si on a un facteur en commun dans $K[X]$, ce facteur est aussi dans $L[X]$, ce qui est absurde. On en déduit l'équivalence souhaitée.
À présent, si pgcd$(P, Q) = D_K$ le pgcd dans $K[X]$ et notons D_L celui dans $L[X]$. Alors, on a $P = D_K P'$ et $Q = D_K Q'$ avec P', Q' deux polynômes de $K[X]$ premiers entre eux sur K donc sur L. On a donc

$$D_L = \text{pgcd}(P, Q) = \text{pgcd}(D_K P', D_K Q') = D_K \text{pgcd}(P', Q') = D_K.$$

On peut aussi s'en convaincre en examinant de près l'algorithme d'Euclide de calcul du pgcd et en constatant qu'il est le même sur $K[X]$ ou sur $L[X]$!

2. Il suffit par exemple de considérer $X^2 + 1$ sur les quaternions $\mathbf{H}$ qui possède trois racines i, j, k.