Feuille TD 2 – Exercices Algèbre – Anneaux – Corrigé Partiel

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

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

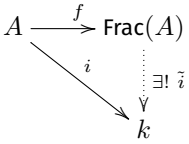
   De même $\frac{ab}{st} = \frac{a'b'}{s't'}$, car

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

   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.

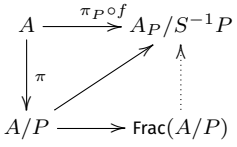
1. Soient $x, y \in \sqrt{I}$. On a alors deux entiers naturels n et m tels que $x^n, y^m \in I$. Ainsi, puisque l'anneau est commutatif,

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

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 $x - y \in I$. Come M est le seul idéal maximal de A on a que l'idéal engendré par $x-y$ est contenu dans M qui est contenu dan s 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.)