Exercice 1.
Soit R un anneau. Parmi les sous-ensembles suivants, lesquels sont-ils des sous-anneaux ?

1. $\{A \in M_n(R) \mid a_{ij} = 0 \text{ si } i > j\} \subset M_n(R)$.
2. $\{A \in M_n(R) \mid a_{ij} = 0 \text{ si } i \leq j\} \subset M_n(R)$.
3. $\{A \in M_n(R) \mid a_{ij} = 0 \text{ si } i \neq j\} \subset M_n(R)$.
4. $\{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.
5. $\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}$.
6. $\left\{\begin{pmatrix} a & b \\ a & b \end{pmatrix} \mid a, b \in \mathbb{Z}\right\} \subset M_2(\mathbb{Z})$.
7. $\left\{\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \mid a, b \in \mathbb{Z}/2\mathbb{Z}\right\} \subset M_2(\mathbb{Z}/2\mathbb{Z})$.

Solution. Puisque nous considérons des sous-ensembles d'anneaux, les propriétés de compatibilité et de distributivité sont automatiquement vérifiées. Il s'agit seulement de vérifier si le sous-ensemble est stable par addition et multiplication, et s'il contient l'élément neutre et le zéro.

1. Les matrices triangulaires supérieures forment un sous-anneau. Les vérifications sont aisées.
2. Ce sous-ensemble ne contient pas la matrice identité.
3. Les matrices diagonales forment un sous-anneau, et les vérifications sont aisées.
4. Cet ensemble (il s'agit de $\mathbb{Z}[i]$) est un sous-anneau. Les vérifications sont aisées.
5. Cet ensemble (il s'agit de $\mathbb{Z}[\sqrt{3}]$) est un sous-anneau. Les vérifications sont aisées.
6. Ce sous-ensemble ne contient pas l'identité.
7. On vérifie par calculs directs que cet ensemble est un sous-anneau.

Exercice 2.
Dans chacun des cas suivants, déterminez l'ensemble des homomorphismes d'anneaux $A \to B$.

1. $A = \mathbb{Z}$ et $B = \mathbb{Z}$.
2. $A = \mathbb{Z}$ et $B = \mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}$.
3. $A = \mathbb{Z}/n\mathbb{Z}$ et $B = \mathbb{Z}$ où $n \in \mathbb{N}$.
4. $A = \mathbb{Z}/m\mathbb{Z}$ et $B = \mathbb{Z}/n\mathbb{Z}$ où $m, n \in \mathbb{N}$.
5. $A = \mathbb{Q}$ et $B = \mathbb{R}$.
6. $A = \mathbb{R}$ et $B = \mathbb{R}$.
7. $A = \mathbb{R}$ et $B = \mathbb{Q}$.
8. $A = \mathbb{R}[t]$ et $B = \mathbb{R}$.
9. $A = \mathbb{R}$ et $B = \mathbb{R}[t]$.

Indication : Pour le point 6, montrez qu'un homomorphisme $f\colon \mathbb{R} \to \mathbb{R}$ envoie les réels positifs vers les réels positifs, et déduisez que f préserve l'ordre usuel sur les réels.

Solution.

1. Si $f\colon \mathbb{Z} \to \mathbb{Z}$ est un homomorphisme, alors
$$f(n) = f(\underbrace{1 + \cdots + 1}_{n \text{ fois}}) = \underbrace{f(1) + \cdots + f(1)}_{n \text{ fois}} = \underbrace{1 + \cdots + 1}_{n \text{ fois}} = n$$
donc $f = \mathrm{Id}_{\mathbb{Z}}$.

2. Le même raisonnement qu'au point précédent donne que, s'il existe un homomorphisme, alors il est donné par $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, s \mapsto [s]_n$. On vérifie sans peine qu'il s'agit bien d'un homomorphisme.

3. Si $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ est un homomorphisme, alors $n \cdot f([1]) = f([n]) = f([0]) = 0$ d'une part, et $n \cdot f([1]) = n \cdot 1 = n \neq 0$ d'autre part, ce qui est une contradiction. Donc il n'existe pas d'homomorphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$.

4. Le même raisonnement qu'au second point donne que, s'il existe un homomorphisme, alors il est donné par $f\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, [s]_m \mapsto [s]_n$. Cependant, cette fonction n'est pas toujours bien définie. Par exemple, si $n = 2$ et $m = 3$, alors on devrait avoir

$$[0]_2 = f([0]_3) = f([1]_3) + f([1]_3) + f([1]_3 = [1]_2 + [1]_2 + [1]_2 = [1]_2,$$

ce qui est absurde.

On prétend que f est bien définie si et seulement si n divise m. Il s'agit d'abord d'une condition nécessaire, puisque

$$[0]_n = f([0]_m) = f(m \cdot [1]_m) = m \cdot f([1]_m) = m \cdot [1]_n = [m]_n.$$

Inversément, supposons que $m = nk$. Alors f est une fonction bien définie, puisque

$$f([s + lm]_m) = [s + lm]_n = [s + lnk]_n = [s]_n = f([s]_m)$$

et l'on vérifie sans peine que f est bien un homomorphisme d'anneaux.

5. Soit $f\colon \mathbb{Q} \to \mathbb{R}$ un homomorphisme. Puisque $f(1) = 1$, on a $0 = f(0) = f(1-1) = 1 + f(-1)$ et donc $f(-1) = -1$. Par additivité on obtient que $f(n) = n$ pour tout $n \in \mathbb{Z}$. Pour $n \in \mathbb{Z}^*$ on a

$$1 = f(1) = f(n \cdot n^{-1}) = n \cdot f(n^{-1})$$

et donc $f(n^{-1}) = n^{-1}$. Par multiplicativité on obtient $f(x) = x$ pour tout $x \in \mathbb{Q}$. Donc f est l'homomorphisme d'inclusion.

6. Soit $f\colon \mathbb{R} \to \mathbb{R}$ un homomorphisme. Par le point précédent, la restriction $f|_{\mathbb{Q}}$ est l'inclusion. Nous allons montrer qu'en fait $f = \mathrm{Id}_{\mathbb{R}}$.

Prenons un nombre réel $x > 0$. Alors il existe un nombre réel y tel que $y^2 = x$. Ainsi $f(x) = f(y^2) = f(y)^2 > 0$. En particulier si $a > b$, alors $f(a) - f(b) = f(a-b) > 0$. Donc f préserve l'ordre usuel sur les réels.

Prenons maintenant un nombre réel x, et choisissons deux suites de nombres rationnels (y_i) et (z_j) tels que $y_i < x < z_j$ pour tous i, j et $\lim_i y_i = x = \lim_j z_j$. Par les observations précédentes, on a

$$y_i = f(y_i) < f(x) < f(z_j) = z_j$$

pour tous i, j. Les conditions sur les limites nous assurent alors, par un simple argument d'analyse, que $f(x) = x$.

7. Il n'existe pas d'homomorphisme $f\colon \mathbb{R} \to \mathbb{Q}$. En effet, si un tel f existait, alors la composition

$$\mathbb{R} \xrightarrow{f} \mathbb{Q} \hookrightarrow \mathbb{R}$$

serait un homomorphisme d'anneaux non-surjectif, en particulier distinct de l'identité, ce qui contredit le point précédent.

8. Par la propriété universelle des anneaux polynomiaux, un homomorphisme $\mathbb{R}[t] \to \mathbb{R}$ est équivalent au choix d'un homomorphisme $\mathbb{R} \to \mathbb{R}$ et d'un élément $a \in \mathbb{R}$ (qui sera l'image de t). En vertu de ce qui précède, on obtient que

$$\mathbb{R} \xrightarrow{1:1} \mathrm{Hom}(\mathbb{R}[t], \mathbb{R}), \quad a \mapsto [p(t) \mapsto p(a)].$$

9. De manière générale, un morphisme d'anneaux doit envoyer un élément inversible vers un élément inversible (la preuve en est aisée). Donc si $f\colon \mathbb{R} \to \mathbb{R}[t]$ est un homomorphisme, tout élément $x \in \mathbb{R}^*$ étant inversible, son image $f(x) \in \mathbb{R}[t]$ est inversible. Or les polynômes inversibles sont les constantes non-nulles. Ainsi f se co-restreint à un homomorphisme $f\colon \mathbb{R} \to \mathbb{R}$, qui est nécessairement l'identité par ce qui précède. Ceci établit que $f\colon \mathbb{R} \to \mathbb{R}[t]$ est l'homomorphisme d'inclusion.

Exercice 3.
Soient A un anneau commutatif et $a \in A$. Montrer que l'application

$$f\colon A[t] \to A[t], \quad p(t) \mapsto p(t+a)$$

est un isomorphisme d'anneaux.

Solution.
Notons tout d'abord que l'application de la donnée est un morphisme d'anneau par la propriété universelle des anneaux de polynômes appliquée à $A \to A[t]$ canonique et l'élément $t+a$. Maintenant l'inverse est donné par

$$A[t] \to A[t], \quad p(t) \mapsto p(t-a),$$

ce qui conclut.

Exercice 4.
Soit G un groupe fini non-trivial. Considérons l'anneau $\mathbb{Z}[G]$.

1. Supposons que $g \in G$ soit non-trivial et que $g^2 = e$. Montrez que $1-g$ et $1+g$ sont des diviseurs de zéro.

2. Plus généralement, montrez que si $g \in G$ est non-trivial, alors $1-g$ est un diviseur de zéro.

Solution.
Notons G multiplicativement, et les éléments de $\mathbb{Z}[G]$ comme des sommes $\sum_{g\in G} a(g)e_g$ où $a(g) \in \mathbb{Z}$. Nous noterons ϵ l'élément neutre de G (donc en particulier $\epsilon = 1$ dans $\mathbb{Z}[G]$).

1. On a que $(1-e_g)(1+e_g) = 1 - e_g + e_g - e_{g^2} = 1 - e_\epsilon = 0$, alors que vu que $g \neq \epsilon$, ni $1-e_g$ ni $1+e_g$ ne sont triviaux.

2. Prenons $g \in G$ distinct de l'élément neutre $\epsilon \in G$. Puisque G est fini et que g n'est pas l'élément neutre, il existe $n > 1$ tel que $g^n = \epsilon$. On a alors :

$$0 = e_\epsilon - e_{g^n} = (e_\epsilon - e_g)(e_\epsilon + e_g + e_{g^2} + \cdots + e_{g^{n-1}})$$

et ni $e_\epsilon - e_g$ ni $e_\epsilon + e_g + \cdots + e_{g^{n-1}}$ ne sont égaux à zéro.

Exercice 5.
Montrez qu'il existe au plus 4 homomorphismes d'anneaux $\mathbb{Z}[S_3] \to \mathbb{Z} \times \mathbb{Z}$.
Indication : si $f\colon \mathbb{Z}[S_3] \to \mathbb{Z} \times \mathbb{Z}$ est un homomorphisme, étudiez les images possibles des éléments de S_3.
($\star$) Montrez qu'il existe exactement 4 morphismes $\mathbb{Z}[S_3] \to \mathbb{Z} \times \mathbb{Z}$.

Solution.

Par souci de clarté, si G est un groupe fini nous écrirons les éléments de $\mathbb{Z}[G]$ sous la forme $\sum_{g\in G} a(g)e_g$, où $a(g) \in \mathbb{Z}$.

Soit $f\colon \mathbb{Z}[S_3] \to \mathbb{Z}\times\mathbb{Z}$ un homomorphisme. Puisque $(123)^3$ est l'élément neutre de S_3, on doit avoir

$$f(e_{(123)})^3 = (1,1).$$

On peut écrire $f(e_{(123)}) = (n,m)$ pour certains $n, m \in \mathbb{Z}$, et donc il faut que $n^3 = m^3 = 1$. Ainsi, on a que

$$f(e_{(123)}) = (1,1).$$

Faisons le même raisonemment pour $e_{(12)}$. Si $f(e_{(12)}) = (a,b)$, alors on obtient que $a^2 = b^2 = 1$, et ainsi (a,b) vaut $(1,1), (1,-1), (-1,1)$ ou $(-1,-1)$.

Puisque (12) et (123) génèrent S_3, la connaissance de $f(e_{(123)})$ et de $f(e_{(12)})$ permet de déterminer f entièrement. On voit donc qu'il existe au plus 4 possibilités pour f.

Pour montrer qu'il existe exactement 4 morphismes, on peut montrer à la main avec les formules qu'envoyer les 2-cycles sur $(a,b) \in \{(1,1),(-1,1),(1,-1),(-1,-1)\}$ et les 3-cycles ainsi que l'élément neutre sur $(1,1)$ se prolonge en unique morphisme. Pour démontrer cela on peut passer par l'argument suivant, qui met en situation ce "prolongement".

L'idée est la suivante: de manière similare au cas des polynômes, la donnée d'un morphisme $R[G] \to S$ pour S un anneau commutatif est *exactement* la même chose que la donnée d'un morphism d'anneaux $R \to S$ et celle d'un morphisme de groupes $G \to (S^\times, \cdot)$. Expliquons cela un peu plus.

Si l'on a un morphisme d'anneaux $f\colon R[G] \to S$, alors on peut précomposer par l'injection canonique $R \to R[G]$ pour obtenir un morphisme d'anneaux $R \to S$. De plus, les éléments de G sont nécessairement envoyés sur des unités de S. En effet, $f(e_g)f(e_{g^{-1}}) = f(e_g e_{g^{-1}}) = f(1) = 1$. Ainsi, on voit que l'on obtient un morphisme de groupes $G \to (S^\times, \cdot)$ donné par $g \mapsto f(e_g)$.

Voyons l'autre sens de la bijection. Si l'on a un morphisme d'anneaux $\theta\colon R \to S$ et un morphisme de groupes $\phi\colon G \to (S^\times, \cdot)$, alors on peut définir $f\colon R[G] \to S$ par

$$f\left(\sum_{g\in G} a(g)e_g\right) = \sum_{g\in G} \theta(a(g))\phi(g) \in S.$$

En utilisant la commutativité de S, on peut montrer que cela est bien un morphisme d'anneaux.

Revenons maintenant à notre cas. On veut comprendre les morphismes d'anneaux $\mathbb{Z}[S_3] \to \mathbb{Z}\times\mathbb{Z}$. Par ce que l'on a dit précédemment, il suffit donc de comprendre les morphismes d'anneaux $\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ et les morphismes de groupes $S_3 \to (\mathbb{Z}\times\mathbb{Z})^\times$.

Pour les morphismes d'anneaux, vu que 1 doit être préservé (et donc ici envoyé sur $(1,1)$), on en déduit par la compatibilité avec l'addition que pour tout $n \in \mathbb{Z}$, son image est obligatoirement $(n,n) \in \mathbb{Z}\times\mathbb{Z}$. Ainsi, il y a bien un unique morphisme d'anneaux $\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ (notez que cet argument montre que pour *tout* anneau R, il y a un unique morphisme $\mathbb{Z} \to R$).

Etudions maintenant les morphisme de groupes $S_3 \to (\mathbb{Z}\times\mathbb{Z})^\times$. Vu que $(\mathbb{Z}\times\mathbb{Z})^\times = \mathbb{Z}^\times \times \mathbb{Z}^\times$ et que $\mathbb{Z}^\times = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$, on en déduit qu'un morphisme de groupes $S_3 \to (\mathbb{Z}\times\mathbb{Z})^\times$ est la même chose que deux morphismes de groups $S_3 \to \mathbb{Z}/2\mathbb{Z}$.

Nous allons montrer qu'il n'y a en fait que 2 tels morphismes (et donc bien quatre morphismes $\mathbb{Z}[S_3] \to \mathbb{Z}\times\mathbb{Z}$ par notre discussion précédente). Donnons deux preuves:

- Vu que $\mathbb{Z}/2\mathbb{Z}$ est abélien, un morphisme $S_3 \to \mathbb{Z}/2\mathbb{Z}$ doit nécessairement contenir $[S_3, S_3] = \langle(123)\rangle$ dans son noyau. Ainsi, il se factorise automatiquement par $S_3/\langle(123)\rangle \cong \mathbb{Z}/2\mathbb{Z}$, et il suffit donc d'étudier les morphismes $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. Il n'y a que deux tels morphismes: le morphisme trivial et l'identité.

- Vu que $(123) \in S_3$ est d'ordre 3, l'ordre de son image doit diviser 3. Etant donné que $\mathbb{Z}/2\mathbb{Z}$ n'a aucun élément d'ordre 3, on obtient que le noyau d'un morphisme $g\colon S_3 \to \mathbb{Z}/2\mathbb{Z}$ doit contenir (123). Ainsi, il se factorise par $S_3/\langle(123)\rangle \cong \mathbb{Z}/2\mathbb{Z}$. On conclut comme juste au-dessus.

Exercice 6.
Soit K un corps et $R \subset K$ un sous-anneau.

1. Montrer que R est intègre.
2. Montrer que si pour tout élément de $k \in K$ il existe $r \in R$ non-nul tel que $rk \in R$, alors l'application naturelle $\mathrm{Frac}(R) \to K$ est un isomorphisme.
3. Les inclusions suivantes sont-elles l'inclusion d'un anneau dans son corps des fractions ?
   (a) $\mathbb{Z}[i] \subset \mathbb{Q}[i]$
   (b) $\mathbb{Z}[t] \subset \mathbb{Q}[t]$
   (c) $R[x,y] \subset K(x,y)$ si $K = \mathrm{Frac}(R)$.

Solution.

1. Si $a, b \in R$ satisfont que $ab = 0$, alors c'est aussi vrai dans K (qui est un corps, donc certainement intègre). Du coup, a ou b doivent être nuls.
2. Nommons cette application θ, et montrons tout d'abord qu'elle est injective. Vu que $\ker(\theta)$ est un idéal de K, on a que soit $\ker(\theta) = \mathrm{Frac}(R)$ ou $\ker(\theta) = 0$. Dans le deuxième cas on est bon, et le premier cas est absurde.

   Si l'on s'évite de parler d'idéaux (c'est le thème de la prochaine série), alors on peut raisonner ainsi: supposons qu'il existe $s \in \mathrm{Frac}(R)^\times$ tel que $\theta(s) = 0$. Alors $1 = \theta(1) = \theta(ss^{-1}) = \theta(s)\theta(s^{-1}) = 0$, et donc on a une contradiction.

   Montrons maintenant la surjectivité: soit $k \in K$, et par hypothèse soit $0 \neq r \in R$ tq $rk \in R$. On a alors que
   $$r\theta\left(\frac{rk}{r}\right) = \theta\left(\frac{rk}{1}\right) = rk,$$
   et donc en divisant par $r \in R \subseteq K$ des deux cotés, on obtient que
   $$\theta\left(\frac{rk}{r}\right) = k.$$
3. (a) C'est le cas. On a vu en cours que $\mathbb{Q}[i]$ est en corps. Maintenant, si $s = \frac{a}{b} + \frac{c}{d}i$, alors $(bd)s \in \mathbb{Z}[i]$.
   (b) Non, car $\mathbb{Q}[t]$ n'est pas un corps (t n'a pas d'inverse).
   (c) C'est le cas. Montrons-le en deux temps. Disons qu'une inclusion d'anneaux intègres $A \subseteq B$ satisfait $(\star)$ si pour tout $b \in B$, alors il existe $a \in A$ non-nul tel que $ab \in A$. Notez que si $A \subseteq B$ et $B \subseteq C$ satisfont $(\star)$, alors $A \subseteq C$ le satisfait aussi.

   Par le point précédent, il suffit de montrer que $R[x,y] \subseteq K(x,y)$ satisfait $(\star)$, et donc que les deux inclusions $R[x,y] \subseteq K[x,y]$ et $K[x,y] \subseteq K(x,y)$ satisfont $(\star)$. Pour la première inclusion, si $f = \sum_{i,j} \frac{r_{ij}}{s_{ij}} x^i y^j \in K[x,y]$ est non-nul, et $s := \prod_{i,j} s_{i,j}$ (il y a un nombre fini de tels éléments par définition d'un polynôme), alors $sf \in R[x,y]$.

   Pour la deuxième inclusion, c'est en fait immédiat parce que $K(x,y)$ est par définition le corps des fractions de $K[x,y]$.

Exercice 7 $(\star)$**.**
Soit k un corps. Considérons l'anneau des séries formelles $k[[t]]$.

1. Montrez que $f(t) = \sum_{i=0}^{\infty} a_i t^i$ est un élément inversible de $k[[t]]$ si et seulement si $a_0 \neq 0$. *Indication : Construisez les inverses algorithmiquement. Le cas de $f(t) = 1 - t$ est instructif pour comprendre la preuve générale.*

2. Montrer que le corps des fractions de $k[[t]]$ est donné par les séries de Laurent

$$k((t)) := \left\{ \sum_{i=n}^{\infty} a_i t^i \mid a_i \in k, n \in \mathbb{Z} \right\}.$$

Solution.

1. Montrons que $f(t) = \sum_{i=0}^{\infty} a_i t^i$ est inversible si et seulement si $a_0 \neq 0$.

   C'est une condition nécessaire : si $g(t) = \sum_{i=0}^{\infty} b_i t^i$ est tel que $f(t)g(t) = 1$, alors $a_0 b_0 = 1$.

   Inversément, supposons $a_0 \neq 0$. Nous allons définir inductivement des coefficients b_i tels que $1 - f(t) \cdot \sum_{i=0}^{n} b_i t^i \in (t^{n+1})$.

   - $b_0 := a_0^{-1}$.
   - Supposons $b_0, \ldots, b_{n-1}$ construits. On a

$$1 - f(t) \cdot \sum_{i=0}^{n} b_i t^i = \underbrace{1 - f(t) \cdot \sum_{i=0}^{n-1} b_i t^i}_{\in (t^n)} - f(t) \cdot b_n t^n$$

     et donc la condition $1 - f(t) \cdot \sum_{i=0}^{n} b_i t^i \in (t^{n+1})$ est équivalente à

$$\sum_{i=0}^{n-1} a_{n-i} b_i = -a_0 b_n.$$

     On prend ainsi $b_n := -a_0^{-1} \sum_{i=0}^{n-1} a_{n-i} b_i$.

   Posons $g(t) := \sum_{i=0}^{\infty} b_i t^i$. Par construction, le terme constant du produit $f(t)g(t)$ vaut 1. On prétend qu'en fait $f(t)g(t) = 1$. Si ce n'est pas le cas, alors il existe un certain $n \geq 1$ tel que $1 - f(t)g(t) \in (t^n)$, et on peut prendre un tel n maximal. Mais par construction

$$1 - f(t)g(t) = \underbrace{\left[1 - f(t) \cdot \sum_{i=0}^{n} b_i t^i\right]}_{\in (t^{n+1})} - \underbrace{t^{n+1} \left[f(t) \cdot \sum_{i=0}^{\infty} b_{i+n+1} t^i\right]}_{\in (t^{n+1})}$$

   donc $1 - f(t)g(t) \in (t^{n+1})$, contradiction puisque n est maximal. Ceci prouve que $g(t) = f(t)^{-1}$.

   Remarquez que même si $f(t)$ est un polynôme, son inverse $f(t)^{-1}$ sera seulement une série formelle. Donc l'anneau $k[t]$ est très différent de l'anneau $k[[t]]$. Cette différence est comparable (dans un sens que nous n'élaborerons pas) à celle qui sépare les fonctions holomorphes définies sur $\mathbb{C}$, de celles qui ne sont définies que sur un voisinage de $0 \in \mathbb{C}$.

   Voici un autre solution, qui s'inspire de la relation

$$(1 - t) \cdot \sum_{i=0}^{\infty} t^i = 1.$$

   Etant donné $g(t) = \sum_{i=0}^{\infty} a_i t^i$, on peut être tenté de remplacer t par $g(t)$ dans la relation ci-dessus, et en déduire que $\sum_{i \geq 0} g(t)^i$ est l'inverse de $1 - g(t)$. Puisque n'importe quelle série

formelle peut s'écrire sous la forme $1 - g(t)$, on aurait montré l'existence d'inverses — pour *tous* les éléments de $k[[t]]$, ce qui est bien sûr absurde. Le problème est que la somme infinie $\sum_{i\geq 0} g(t)^i$ n'est pas forcément bien définie (par exemple si $g(t) = \lambda \in k^*$). En fait, on vérifie aisément que cette somme infinie n'a de sens que si $g(t)$ n'a pas de terme constant, auquel cas le terme de degré n de cette série se définit comme le terme de degré n de la somme finie $1 + g(t) + \cdots + g(t)^n$.

Ceci étant dit, soit $f(t)$ une série possédant un terme constant. Si $\lambda \in k^*$, alors il est équivalent de trouver un inverse de $f(t)$ et de trouver un inverse de $\lambda f(t)$. Donc on peut supposer que le terme constant de $f(t)$ vaut 1. Dans ce cas $F(t) := 1 - f(t)$ n'a pas de terme constant, la somme infinie $\sum_{i\geq 0} F(t)^i$ peut être définie, et nous allons vérifier qu'il s'agit bien d'un inverse de $f(t)$. La vérification est semblable à ce qui a été fait précédemment : le terme constant de $f(t) \cdot \sum_{i=0}^{\infty} F(t)^i$ vaut 1, donc si ce produit ne vaut pas 1 il existe un $N > 0$ maximal tel que

$$1 - f(t) \cdot \sum_{i=0}^{\infty} F(t)^i \in (t^N).$$

Or

$$\begin{aligned} 1 - f(t) \cdot \sum_{i=0}^{\infty} F(t)^i &= 1 - (1 - F(t)) \cdot \sum_{i=0}^{N} F(t)^i + t^{N+1} f(t) \sum_{i=N+1}^{\infty} \frac{F(t)^i}{t^{N+1}} \\ &= 1 - (1 - F(t)^{N+1}) + t^{N+1} f(t) \sum_{i=N+1}^{\infty} \frac{F(t)^i}{t^{N+1}} \\ &= F(t)^{N+1} + t^{N+1} f(t) \sum_{i=N+1}^{\infty} \frac{F(t)^i}{t^{N+1}} \\ &\in (t^{N+1}) \end{aligned}$$

ce qui est une contradiction. Donc $f(t)^{-1} = \sum_{i=0}^{\infty} F(t)^i$.

2. Montrons d'abord que $k((t))$ est un corps. Il est facile de vérifier qu'il s'agit d'un anneau commutatif intègre (avec les opérations évidentes — la multiplication est définie de la même manière que dans $k[[t]]$), et que $k[[t]]$ est un sous-anneau de $k((t))$. Prenons $0 \neq f(t) = \sum_{i\geq n} a_i t^i \in k((t))$, où l'on fait la convention que $a_n \neq 0$. Alors $t^{-n} f(t) = \sum_{i\geq 0} a_{i+n} t^i \in k[[t]]$ est un élément inversible par le premier point, donc il existe $g(t) \in k[[t]]$ tel que $t^{-n} f(t) g(t) = 1$. On en déduit que $t^{-n} g(t) \in k((t))$ est l'inverse de $f(t)$. Donc $k((t))$ est bien un corps.

   Montrons maintenant que chaque élément de $k((t))$ peut s'écrire comme un ratio d'éléments de $k[[t]]$. Considérons à nouveau $0 \neq f(t) = \sum_{i\geq n} a_i t^i$. Si $n \geq 0$ alors $f(t) \in k[[t]]$. Si $n < 0$, alors $t^{-n} f(t) = h(t) \in k[[t]]$ et ainsi

$$f(t) = \frac{h(t)}{t^{-n}}$$

   où le numérateur et le dénominateur appartiennent à $k[[t]]$.