EPFL - Printemps 2023 | Prof. Z. Patakfalvi
Anneaux et Corps | **Exercices**
Solutions 1

Exercice 1.
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.
Notons G multiplicativement, et les éléments de $\mathbb{Z}[G]$ comme des sommes $\sum_{g\in G} a(g)e_g$ où $a(g) \in \mathbb{Z}$. 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 $e_\epsilon + e_g + \cdots + e_{g^{n-1}}$ n'est égal à zéro.

Exercice 3. 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 $n \cdot f([1]) = n \cdot 1 = n$ 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 4.
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 $f\colon \mathbb{Z}[S_3] \to \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ un homomorphisme. Puisque $(123)^3$ est l'élément neutre de S_3, on doit avoir

$$f(e_{(123)})^3 = e_0.$$

On peut écrire $f(e_{(123)}) = ne_0 + me_1$ pour certains $n, m \in \mathbb{Z}$. Puisque $\mathbb{Z}/2\mathbb{Z}$ est un groupe commutatif, son algèbre de groupe sur $\mathbb{Z}$ est un anneau commutatif. On calcule donc

$$(ne_0 + me_1)^3 = (n^3 + 3nm^2)e_0 + (m^3 + 3n^2m)e_1.$$

Ainsi $m(m^2+3n^2) = 0$ et $n(n^2+3m^2) = 1$. Si $m = 0$ alors $n = 1$; si $m^2+3n^2 = 0$ alors $m = 0 = n$, ce qui n'est pas possible en vue de la seconde condition. On a donc montré que $f(e_{(123)}) = e_0$.

Faisons le même raisonemment pour $e_{(12)}$. Si $f(e_{(12)}) = ae_0 + be_1$, alors on obtient

$$e_0 = (a^2 + b^2)e_0 + 2abe_1$$

et donc (a, b) vaut $(0, 1), (0, -1), (1, 0)$ ou $(-1, 0)$.

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 ae_0+be_1 pour $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$ et les 3-cycles ainsi que l'élément neutre sur e_0 se prolonge en unique morphisme. Pour démontrer cela on peut passer par l'argument suivant, qui met en situation ce "prolongement".

On remarque que $\mathbb{Z}[-]$: Grp $\to$ Ring si Grp désigne la catégorie des groupes et Ring la catégorie des anneaux (non nécessairement commutatifs) est adjoint à gauche de $(A, +, \cdot) \mapsto (A^\times, \cdot)$. Notez également que l'abélianisé de S_3 est $\mathbb{Z}/2\mathbb{Z}$. Dès lors, en utilisant l'adjonction ci-dessus et l'adjonction abélianisé $\dashv$ oubli entre Ab et Grp on obtient

$$\begin{aligned}&\mathrm{Hom}_{\mathrm{Ring}}(\mathbb{Z}[S_3], \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]) \cong \mathrm{Hom}_{\mathrm{Grp}}(S_3, \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]^\times)\\ &\cong \mathrm{Hom}_{\mathrm{Ab}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]^\times)\end{aligned}$$

ce qui conclut car le calcul au-dessus démontre que les seuls éléments $a \in \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]^\times$ tel que $a^2 = 1$ sont $ae_0 + be_1$ pour $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$.

Exercice 5.
Par souci de clarté, notons n_A l'élément $\underbrace{1_A + \cdots + 1_A}_{n \text{ fois}} \in A$.

1. Puisque $a \in A$ génère le groupe additif, tout élément de A peut s'écrire comme une somme $a + \cdots + a$. Par distributivité on a

$$(\underbrace{a + \cdots + a}_{n \text{ fois}}) \cdot (\underbrace{a + \cdots + a}_{m \text{ fois}}) = \underbrace{a^2 + \cdots + a^2}_{nm \text{ fois}} = (\underbrace{a + \cdots + a}_{m \text{ fois}}) \cdot (\underbrace{a + \cdots + a}_{n \text{ fois}}).$$

   Donc A est commutatif.

2. Il découle du calcul précédent que la connaissance de a^2 détermine la multiplication de A.

3. Puisque a génère A additivement, il existe $s \geq 1$ tel que

$$s_A \cdot a = \underbrace{a + \cdots + a}_{s \text{ fois}} = 1_A$$

   et donc s_A est un inverse à gauche de a. Puisque A est commutatif, s_A est aussi un inverse à droite et ainsi $a^{-1} = s_A$.

4. Il existe un $t \geq 1$ tel que $t_A \cdot a = a^2$. On a alors

$$a = a \cdot a \cdot a^{-1} = a^2 \cdot a^{-1} = t_A \cdot a \cdot a^{-1} = t_A \cdot 1_A.$$

En particulier 1_A génère aussi le groupe additif $(A, +)$. Puisque A est d'ordre n, on a nécessairement $A = \{0_A, 1_A, 2_A, \ldots, (n-1)_A\}$. Ceci permet de définir

$$f \colon \mathbb{Z}/n\mathbb{Z} \to A, \quad [r]_n \mapsto r_A$$

car $r_A + (nk)_A = r_A$. Il est clair qu'il s'agit un homomorphisme bijectif, donc d'un isomorphisme.

Exercice 6.
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 7.
On utilise la notation suivante (symbole delta de Kronecker) : $\delta^i_j = 0$ si $i \neq j$, et $\delta^i_i = 1$.

1. Soient $A = (a_{ij}), B = (b_{ij}) \in M(k)$. L'addition est donnée par

$$(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij})$$

et la multiplication par

$$(a_{ij}) \cdot (b_{ij}) := \left(\sum_{k=1}^{\infty} a_{ik} b_{kj} \right)_{i,j \in \mathbb{N}}$$

La multiplication est bien définie, puisque la condition de finitude assure que la série est en fait une somme finie. Pour montrer que chaque colonne du produit est à support fini, prenons un indice j quelconque. Soit N suffisamment grand tel que pour tous les indices $i \geq N$ on a $b_{ij} = 0$. Maintenant si M est suffisamment grand pour que pour tout $i \geq M$ et tout les $j \leq N$ on a $a_{ij} = 0$, on obtient que si $i \geq M$ que $(A \cdot B)_{ij} = 0$. L'associativité, la distributivité et autres propriétés des axiomes d'anneaux sont facilement. vérifiées, ce sont les même calculs que dans le cas fini. La matrice nulle est l'élément neutre additif et la matrice $(a_{ij} = \delta^i_j)$ est l'élément neutre multiplicatif. Donc $M(k)$ est un anneau.

2. Prenons

$$A := \left(a_{ij} = \delta^i_{j+1}\right)_{i,j}, \quad B := \left(b_{ij} = \delta^{i+1}_j\right)_{i,j},$$

ce sont des éléments de $M(k)$. Visuellement, on peut se représenter A comme la matrice identité dont on a décalé la diagonale d'une ligne vers le bas — et B comme la matrice identité dont on a décalé la diagonale d'une colonne vers la droite.

On vérifie alors que $BA = 1_{M(k)} \neq AB$. Cela implique que A n'a pas d'inverse à droite : car s'il existait B' tel que $AB' = 1_{M(k)}$, alors $B = BAB' = B'$.

Remarque. On peut également remarquer que cet anneau de matrices est isomorphe à l'anneau des endomorphismes k-linéaires de $k^{\oplus \mathbb{N}}$. Dès lors si on représente les éléments de cet espace comme des vecteurs à support fini d'éléments de k écrits de gauche à droite la matrice A correspond au décalage d'un cran vers la droite avec zéro en première composante et B au décalage d'un cran vers la gauche.

Exercice 8. 1. Un anneau A intègre et fini est un corps. En effet, prenons $a \neq 0$ et considérons la fonction

$$A \to A, \quad x \mapsto ax.$$

Puisque $a \neq 0$ et que A est intègre, cette fonction est injective. Mais A est un ensemble fini, donc cette fonction est en fait bijective. Ainsi il existe un $y \in A$ tel que $ay = 1$. Le même raisonnement appliqué à la fonction $x \mapsto xa$ donne un $y' \in A$ tel que $y'a = 1$. Ainsi $y = y'ay = y'$, et $a^{-1} = y$. Donc A est un corps.

On peut aussi montrer que si A est un anneau fini sans diviseur de zéro, alors A est nécessairement un corps (commutatif), mais cela est bien moins facile — il s'agit du (petit) théorème de Wedderburn.

2. Un anneau A dans lequel $x = x^2$ pour tout $x \in A$, est commutatif. En effet, prenons $a, b \in A$. On a alors

$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + b + ab + ba$$

et ainsi $ab = -ba$. Or $-1 = (-1)^2 = 1$, donc $ab = -ba = ba$, comme désiré.

Les anneaux qui vérifient cette condition sont appelés *algèbres booléennes*. Elles ont des liens surprenants avec la topologie et la logique mathématique. Voir *dualité de Stone* sur wikipedia ou sur le n-lab.

Exercice 9. 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 $k[[t]]$.