EPFL - Printemps 2022	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 2	

Exercice 1. (a) $1 \notin B$, therefore B is not a subring of A. On the other hand, B is a bilateral ideal in A (Definition 1.4.4).

(b) $[1] \notin B$, hence B is not a subring of A and, as A is a field, B is neither an ideal in A.

(c) $1 \notin B$, therefore B is not a subring of A. For $t \in A$ and $t^2 \in B$ we have that $t \cdot t^2 = t^3 \notin B$, hence B is not a left ideal in A and moreover, as A is commutative, B is neither a right ideal.

(d) $[1] \notin B$, therefore B is not a subring of A. Let $f(t) \in A$ and let $t^2 g(t) \in B$, for some $g(t) \in A$. Then $f(t) \cdot (t^2 g(t)) = t^2(f(t)g(t)) \in B$ and thus B is a left ideal in A. Furthermore, as A is commutative, B is a bilateral ideal.

(e) $B \not\subseteq A$.

(f) $B \not\subseteq A$.

(g) $[1] \notin B$, therefore B is not a subring of A. Moreover, as $B = ([5])$, B is a bilateral ideal of A.

(h) B is the set of lower triangular matrices in $M_n(\mathbb{R})$, hence it is a subgring of A. If $n > 1$ then B is not an ideal of A. if $n = 1$ then $B = A$ and we conclude that B is a bilateral ideal in A.

(i) If $n = 0$ then $A = B$ and thus B is both a subring and a bilateral ideal of A. If $n > 0$, then $1 \notin B$,hence B is not a subring of A, but, on the other hand, as $B = (p^n)$, we have that B is a bilateral ideal of A.

(j) $\mathrm{I}_3 \notin B$, hence B not a subring. Since

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ a & b & 0 \end{pmatrix} \notin B,$$

it follows that B is not a left ideal in A. Similarly, as

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & b \\ 0 & 0 & d \\ 0 & 0 & 0 \end{pmatrix} \notin B,$$

it follows that B is also not a right ideal in A.

(k) B is a subring of A: we have that $\mathrm{I}_3 \in B$, $(B, +)$ is a subgroup of $M_n(\mathbb{R})$ and B is stable under matrix multiplication. As $B \neq A$ and $\mathrm{I}_3 \in B$, it follows that B is neither a left nor a right ideal of A.

(l) $\mathrm{I}_3 \notin B$, hence B is not a subring of A. We check to see if B is a left ideal in A. For this let $A = (a_{ij}) \in A$ and we have

$$A \begin{pmatrix} a & a & 0 \\ b & b & 0 \\ c & c & 0 \end{pmatrix} = \begin{pmatrix} a_{11}a + a_{12}b + a_{13c} & a_{11}a + a_{12}b + a_{13c} & 0 \\ a_{21}a + a_{22}b + a_{23c} & a_{21}a + a_{22}b + a_{23c} & 0 \\ a_{31}a + a_{32}b + a_{33c} & a_{31}a + a_{32}b + a_{33c} & 0 \end{pmatrix} \in B.$$

Therefore B is a left ideal of A. On the other hand, B is not a right ideal as

$$\begin{pmatrix} 1 & 1 & 0 \\ 2 & 2 & 0 \\ 3 & 3 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 3 & 0 & 0 \end{pmatrix} \notin B.$$

(m) B is not a subring of A as $\mathrm{Id} \notin B$. Let $a = a_0 \mathrm{Id} + a_1(12) + a_2(13) + a_3(23) + a_4(123) + a_5(132) \in A$ and let $b = \lambda[\mathrm{Id} + (12) + (13) + (23) + (123) + (132)] \in B$. Then

$$a \cdot b = b \cdot a = \lambda(a_0 + a_1 + a_2 + a_3 + a_4 + a_5) \sum_{g \in S_3} g \in B$$

and we deduce that B is a bilateral ideal of A.

(n) Again, B is not a subring of A, as $\mathrm{Id} \notin B$. Let $a = a_0 \mathrm{Id} + a_1(12) + a_2(13) + a_3(23) + a_4(123) + a_5(132) \in A$ and let $b = \lambda \mathrm{Id} - \lambda(12) - \lambda(13) - \lambda(23) + \lambda(123) + \lambda(132) \in B$. One checks that

$$\begin{aligned} a \cdot b = {} & \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5) \mathrm{Id} - \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5)(12) - \\ & - \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5)(13) - \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5)(23) + \\ & + \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5)(123) + \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5)(132) \\ = {} & \sum_{g \in S_3} (-1)^{\mathrm{sgn}(g)} \mu \cdot g, \end{aligned}$$

where $\mu = \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5) \in \mathbb{C}$. Therefore B is a left ideal of A. Analogously, one shows that:

$$b \cdot a = \sum_{g \in S_3} (-1)^{\mathrm{sgn}(g)} \mu \cdot g,$$

where $\mu = \lambda(a_0 - a_1 - a_2 - a_3 + a_4 + a_5) \in \mathbb{C}$, and therefore B is a bilateral ideal of A.

(o) Again, B is not a subring of A, as $\mathrm{Id} \notin B$. Let $a = a_0 \mathrm{Id} + a_1(12) + a_2(13) + a_3(23) + a_4(123) + a_5(132) \in A$ and let $b = \lambda \mathrm{Id} + \lambda\varepsilon(123) + \lambda\varepsilon^2(132) + \mu(12) + \mu\varepsilon(23) + \mu\varepsilon^2(13) \in B$. We compute:

$$\begin{aligned} a \cdot b = {} & (\lambda a_0 + \mu a_1 + \mu\varepsilon^2 a_2 + \mu\varepsilon a_3 + \lambda\varepsilon^2 a_4 + \lambda\varepsilon a_5) \mathrm{Id} + (\lambda\varepsilon a_0 + \mu\varepsilon a_1 + \mu a_2 + \mu\varepsilon^2 a_3 + \lambda a_4 + \\ & + \lambda\varepsilon^2 a_5)(123) + (\lambda\varepsilon^2 a_0 + \mu\varepsilon^2 a_1 + \mu\varepsilon a_2 + \mu a_3 + \lambda\varepsilon a_4 + \lambda a_5)(132) + (\mu a_0 + \lambda a_1 + \\ & + \lambda\varepsilon a_2 + \lambda\varepsilon^2 a_3 + \mu\varepsilon a_4 + \mu\varepsilon^2 a_5)(12) + (\mu\varepsilon a_0 + \lambda\varepsilon a_1 + \lambda\varepsilon^2 a_2 + \lambda a_3 + \mu\varepsilon^2 a_4 + \mu a_5)(23) + \\ & + (\mu\varepsilon^2 a_0 + \lambda\varepsilon^2 a_1 + \lambda a_2 + \lambda\varepsilon a_3 + \mu a_4 + \mu\varepsilon a_5)(13) \end{aligned}$$

Set $x = \lambda a_0 + \mu a_1 + \mu\varepsilon^2 a_2 + \mu\varepsilon a_3 + \lambda\varepsilon^2 a_4 + \lambda\varepsilon a_5$ and $y = \mu a_0 + \lambda a_1 + \lambda\varepsilon a_2 + \lambda\varepsilon^2 a_3 + \mu\varepsilon a_4 + \mu\varepsilon^2 a_5$. Then, $x, y \in \mathbb{C}$ and we see that

$$a \cdot b = x \mathrm{Id} + x\varepsilon(123) + x\varepsilon^2(132) + y(12) + y\varepsilon(23) + y\varepsilon^2(13) \in B$$

and conclude that B is a left ideal of A.

On the other hand, let $a = a_0 \mathrm{Id} + a_1(12) \in A$ and $b = \lambda \mathrm{Id} + \lambda\varepsilon(123) + \lambda\varepsilon^2(132) + \mu(12) + \mu\varepsilon(23) + \mu\varepsilon^2(13) \in B$. Then:

$$\begin{aligned} b \cdot a = {} & (\lambda a_0 + \mu a_1) \mathrm{Id} + \varepsilon(\lambda a_0 + \mu\varepsilon a_1)(123) + \varepsilon^2(\lambda a_0 + \mu\varepsilon^2 a_1)(132) + (\mu a_0 + \lambda a_1)(12) + \\ & + \varepsilon(\mu a_0 + \lambda\varepsilon a_1)(23) + \varepsilon^2(\mu a_0 + \lambda\varepsilon^2 a_1)(13) \notin B. \end{aligned}$$

Hence B is not a right ideal of A.

(p) Once more, B is not a subring of A, as $\mathrm{Id} \notin B$. One checks that:

$$\begin{cases} (12) \cdot [\lambda(123) + \lambda(132)] = \lambda(23) + \lambda(13) \notin B \\ [\lambda(123) + \lambda(132)] \cdot (12) = \lambda(13) + \lambda(23) \notin B \end{cases},$$

hence B is neither a left, nor a right ideal of A.

Exercice 2. 1. Let $A = (a_{ij}) \in M_n(K)$ be a matrix which is concentrated in the j^{th} column, i.e. $a_{rs} = 0$ for all $s \neq j$. For all $1 \leq r \leq n$ consider the matrix $B_r = a_{rj} e_{ri} \in M_n(K)$. Then $B_r e_{ij} \in I$, where

$$(B_r e_{ij})_{kl} = \sum_{m=1}^{n} (a_{rj} e_{ri})_{km} (e_{ij})_{ml} = a_{rj} \sum_{m=1}^{n} \delta_{rk} \delta_{im} \delta_{jl} = a_{rj} \delta_{rk} \delta_{jl} = \begin{cases} a_{rj}, & \text{if } k = r \text{ and } l = j \\ 0, & \text{otherwise} \end{cases} .$$

Lastly, as $A = \sum_{r=1}^{n} (B_r e_{ij})$, we conclude that $A \in I$.

2. Let $S \subseteq M_n(K)$ be the subset of matrices which are concentrated in the j^{th} column. Clearly, S is an additive subgroup of $M_n(K)$. Now, let $A = (a_{rs}) \in M_n(K)$ and let $B = (b_{rs}) \in S$. As

$$(A \cdot B)_{rs} = \sum_{m=1}^{n} a_{rm} b_{ms},$$

it follows that $(A \cdot B)_{rs} = 0$ for all $s \neq j$, and we deduce that $A \cdot B \in S$. Therefore, S is a left ideal in $M_n(K)$.

3. Let $\{0\} \neq I$ be a bilateral ideal in $M_n(K)$. Let A be a non-zero matrix in I. Then A admits a non-zero coefficient a_{ij}. As I is an ideal and K is a field we have that $\frac{1}{a_{ij}} \mathrm{I}_n \cdot A \in I$ and so, we can assume without loss of generality that $a_{ij} = 1$. Since I is a bilateral ideal, it follows that for all $1 \leq r, s \leq n$, the product $e_{ri} A e_{js} \in I$. We compute

$$\begin{aligned}(e_{ri} A e_{js})_{kl} &= \sum_{q=1}^{n} (e_{ri} A)_{kq} (e_{js})_{ql} = \sum_{q=1}^{n} \Big[\sum_{p=1}^{n} (e_{ri})_{kp} a_{pq}\Big] \delta_{jq} \delta_{sl} = \sum_{p=1}^{n} \delta_{rk} \delta_{ip} a_{pj} \delta_{sl} \\ &= \delta_{rk} a_{ij} \delta_{sl} = \delta_{rk} \delta_{sl} = (e_{rs})_{kl}\end{aligned}$$

and it follows that $e_{rs} \in I$ for all $1 \leq r, s \leq n$. Lastly, as I is an additive subgroup of $M_n(K)$, we conclude that $I = M_n(K)$.

Exercice 3. (a) Let $0 \neq x \in I$ and let $0 \neq y \in J$. Then $xy \neq 0$, as A is integral, and $xy \in I \cap J$;

(b) Proposition 1.4.6;

(c) Exercice 2;

(d) Proposition 1.4.6.

Pour les points (e) et (f), l'argument suivant s'applique. Soit $x \in K$ non-nul. Alors $Kx = K$. En particulier, il existe $y \in K$ tel que $yx = 1$. Comme $Ky = K$, il existe $z \in K$ tel que $zy = 1$. En multipliant par x à droite, on obtient, $zyx = x$, et donc $z = x$. Ainsi y est un inverse à droite et à gauche de x.

Exercice 4. (a) Example 1.4.9;

(b) Recall the quotient homomorphism $\xi : A \to A/I$ given by $a \xrightarrow{\xi} [a]$ (Proposition 1.4.13). This induces the surjective ring homomorphism $f : M_n(A) \to M_n(A/I)$ given by $(a_{ij}) \xrightarrow{\mathrm{f}} ([a_{ij}])$. The kernel of f consists of those matrices in $M_n(A)$ whose coefficients are zero in A/I, hence $\ker(f) = M_n(I)$. We conclude that $M_n(A)/M_n(I) \cong M_n(A/I)$.

(c) Let $\varphi : \mathbb{Z} \to \mathbb{Z}[\sqrt{7}]/I$, where $\varphi(n) = [n]$, for all $n \in \mathbb{Z}$. Clearly, φ is a ring homomorphism and $\ker(\varphi) = \{n \in \mathbb{Z} \mid n \in I\}$. Let $n \in \ker(\varphi)$. Then there exist $a, b \in \mathbb{Z}$ such that $n = (5+2\sqrt{7})(a+b\sqrt{7})$. We make the computations and arrive at $2n = 3b$. As $\gcd(2,3) = 1$, we have $n \in (3)$, hence $\ker(\varphi) \subseteq (3)$. Conversely, let $n \in (3)$. Then $n = 3m$, for some $m \in \mathbb{Z}$, and $\varphi(n) = \varphi(3)\varphi(m) = 0$. We deduce that $\ker(\varphi) = (3)$.

The only thing left to prove is that φ is surjective. Before we proceed, we remark that $\sqrt{7}(5+2\sqrt{7}) = 14 + 5\sqrt{7} \in I$ and $(14+5\sqrt{7}) - 2(5+2\sqrt{7}) = 4 + \sqrt{7} \in I$. Now, let $[a + b\sqrt{7}] \in \mathbb{Z}[\sqrt{7}]/I$. We have that

$$[a+b\sqrt{7}] = [a] + [b\sqrt{7}] = [a] + [-4b] = \varphi(a) + \varphi(-4b) = \varphi(a-4b).$$

We use the isomorphism theorem to conclude that $\mathbb{Z}/(3) \cong \mathbb{Z}[\sqrt{7}]/(5+2\sqrt{7})$.

Exercice 5.
We recall that, by convention, the degree of the zero polynomial is $-\infty$ and that $-\infty + n = -\infty$ for all positive integers n. We can therefore assume that $f, g \neq 0$. We write $f(t) = \sum_{i=0}^{m} a_i t^i$, where $a_m \neq 0$, hence $\deg(f) = m$, and $g(t) = \sum_{j=0}^{n} b_j t^j$, where $b_n \neq 0$, hence $\deg(g) = n$. Now $f(t)g(t) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_i b_j t^{i+j}$ and so $\deg(fg) = n + m$, as the leading coefficient of fg is $a_m b_n \neq 0$, by integrity of A.

Exercice 6.
Consider the evaluation homomorphism $\mathrm{ev}_\varepsilon : \mathbb{Z}[t] \to \mathbb{Z}[\varepsilon]$. Clearly ev_ε is surjective and so, the only thing we need to show is that $(t^2+t+1) = \ker(\mathrm{ev}_\varepsilon)$.

Let $f(t) \in (t^2+t+1)$. Then $f(t) = (t^2+t+1)g(t)$ for some $g(t) \in \mathbb{Z}[t]$ and we have

$$\mathrm{ev}_\varepsilon(f(t)) = \mathrm{ev}_\varepsilon(t^2+t+1)\,\mathrm{ev}_\varepsilon(g(t)) = 0.$$

Therefore $(t^2+t+1) \subseteq \ker(\mathrm{ev}_\varepsilon)$.

Conversely, let $f(t) \in \ker(\mathrm{ev}_\varepsilon)$. We will show that $f(t) \in (t^2+t+1)$ by recurrence on $\deg(f)$.

If $\deg(f) = 0$, then $f(t) = a_0$ and as $\mathrm{ev}_\varepsilon(f) = 0$, it follows that $f = 0$.

If $\deg(f) = 1$, then $f(t) = a_1 t + a_0$, for some $a_1, a_0 \in \mathbb{Z}$, and, as $\mathrm{ev}_\varepsilon(f(t)) = 0$, it follows that $a_1 = a_0 = 0$, hence $f(t) = 0$.

We can now assume that $\deg(f) \geq 2$. We write $f(t) = \sum_{i=0}^{m} a_i t^i$, where $\deg(f) = m$ and $a_i \in \mathbb{Z}$. Then, as $f(t) \in \ker(\mathrm{ev}_\varepsilon)$ and $a_m t^{m-2}(t^2+t+1) \in \ker(\mathrm{ev}_\varepsilon)$, it follows that:

$$g(t) = f(t) - a_m t^{m-2}(t^2+t+1) = \sum_{i=0}^{m-3} a_i t^i + (a_{m-2} - a_m)t^{m-2} + (a_{m-1} - a_m)t^{m-1} \in \ker(\mathrm{ev}_\varepsilon).$$

Now $\deg(g(t)) \leq m-1$ and so, by recurrence, we have $g(t) \in (t^2+t+1)$. Consequently, $f(t) = g(t) + a_m t^{m-2}(t^2+t+1) \in (t^2+t+1)$ and so $\ker(\mathrm{ev}_\varepsilon) = (t^2+t+1)$.

We now apply the isomorphism theorem to conclude that $\mathbb{Z}[t]/(t^2+t+1) \cong \mathbb{Z}[\varepsilon]$.

Exercice 7.
On dit qu'un élément $r \in R$ est *nilpotent* si $r^n = 0$ pour un $n \geq 1$.

On commence par démontrer le fait suivant valide dans n'importe quel anneau commutatif A : si $\lambda \in A^\times$ et $n \in A$ nilpotent, alors $\lambda - n$ est inversible. En effet,

$$\frac{1}{\lambda - n} = \frac{1}{\lambda}\sum_{i=0}^{\infty}(n/\lambda)^i.$$

Ainsi, on voit que tout polynôme $f(t) = \sum_{i=0}^{m} a_i t^i \in R[t]$ avec coefficient constant inversible et tout les autres coefficients nilpotents est inversible. En effet, dans ce cas on peut écrire $f(t) = \tilde{f}(t) - a_0$, avec $\tilde{f}(t)$ un polynôme dont tout les coefficients sont nilpotents. Comme il suit de la formule du binôme qu'une somme d'éléments nilpotents est un élément nilpotent, on voit que $\tilde{f}(t)$ est nilpotent.

Dans ce qui suit, on montre qu'un polynôme inversible est forcément de cette forme.

Soit $f(t) \in (R[t])^\times$. Notons encore $f(t) = \sum_{i=0}^{m} a_i t^i$. On remarque tout d'abord avec $\mathrm{ev}_0 : R[t] \to R$ que $a_0 \in R^\times$. On montre dans ce qui suit que a_i est nilpotent pour $i > 0$. Pour montrer cela, on suppose sans perte de généralité que $a_0 = 1$. On note alors $f(t) = 1 - tg(t)$, et on cherche à démontrer que tout les coefficients du polynôme $g(t)$ sont nilpotents.

On considère l'inclusion $R[t] \subset R[[t]]$. L'inverse de $f(t) = 1 - tg(t)$ dans $R[[t]]$ est (voir remarque après la preuve)

$$\sum_{i=0}^{\infty} t^i (g(t))^i.$$

En effet,

$$(1 - tg(t))\left(\sum_{i=0}^{\infty} t^i (g(t))^i\right) = \sum_{i=0}^{\infty} t^i (g(t))^i - \sum_{i=1}^{\infty} t^i (g(t))^i = 1.$$

Comme on suppose que $f(t)$ est inversible dans $R[t]$, cet élément est en fait un polynôme, *i.e.* il existe $I \in \mathbb{N}$ tel que pour tout $i \geq I$ on a $t^i(g(t))^i = 0$. Comme t n'est pas un diviseur de zéro, on a même $(g(t))^i = 0$ pour tout $i \geq I$. En particulier, on voit que le coefficient dominant a_m est nilpotent. Maintenant, on peut appliquer l'argument qu'on vient d'appliquer pour $f(t)$ au polynôme $h(t) = f(t) - a_m t^m$ pour conclure que a_{m-1} est nilpotent. Par récurence descendante avec le même procédé, on conclut que tout les coefficients de $g(t)$ sont nilpotents.

Remarque. Pour faire sens de toute somme infinie avec $g(t)$ un polynôme

$$\sum_{i=0}^{\infty} t^i (g(t))^i$$

on laisse le soin au lecteur de vérifier que l'application naturelle $R[[t]] \cong \varprojlim_{n\geq 1} R[t]/(t^n)$ est un isomorphisme, où le terme à droite est,

$$\varprojlim_{n\geq 1} R[t]/(t^n) = \{(f_n(t)) \in \prod_{n\geq 1} R[t]/(t^n) \mid f_{n+1}(t) \equiv f_n(t) \mod t^n \quad \forall n \geq 1\} \subseteq \prod_{n\geq 1} R[t]/(t^n)$$

Ainsi, pour définir un élément de $R[[t]]$ il suffit de le faire de manière compatible dans $R[t]/(t^n)$ pour $n \geq 1$. En particulier la collection indicée par $n \geq 1$,

$$f_n(t) = \sum_{i=0}^{n-1} t^i (g(t))^i \mod t^n$$

défini bel et bien un élément de $R[[t]]$.

Exercice 8. 1. On a $\nu(1) = \nu(1^2) = 2\nu(1)$, donc $\nu(1) = 0$. Comme $0 = \nu(1) = \nu(-1^2) = 2\nu(-1)$, on a également $\nu(-1) = 0$.

2. La stabilité de R_ν par l'addition et la multiplication est assurée par a) et b).

3. Immédiat car si $k \in K$, soit k ou k^{-1} est dans R_ν.
4. Comme $\nu(1) = \nu(-1) = 0$, cela suit par b) par récurrence.
5. Suit par la décomposition en nombres premiers et a).
6. Notons d'abord que pour tout $n \in \mathbb{Z}$ et $q \in \mathbb{Q}$. Alors $\nu(nq) \geq \nu(q)$ par a) et le point 4. Si p et q deux premiers distincts avec $\nu(p), \nu(q)$ non-nuls, alors comme par Bézout il existe $a, b \in \mathbb{Z}$ tel que $ap + bq = 1$,

   $$0 = \nu(1) = \nu(ap + bq) \geq \min(\nu(ab), \nu(bq)) \geq \min(\nu(p), \nu(q)) > 0$$

   une contradiction.
7. Cela suit par a) si on note $c = \nu(p)$ et le point précédent.
8. Si q est un premier distinct de p, alors $q^{-1} \in R_{\nu_p}$.