Exercice 1.
Dans chacun des cas suivants, déterminer si l'affirmation suivante est vraie ou fausse. Justifier la réponse par un raisonnement ou un contre-exemple.

1. L'image d'un idéal bilatère par un homomorphisme d'anneaux est encore un idéal bilatère.
2. La préimage d'un idéal bilatère par un homomorphisme d'anneaux est encore un idéal bilatère.

Solution.

1. Wrong, for example, one can see that for the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$, the image of the ideal $(2) \subseteq \mathbb{Z}$ is not an ideal in $\mathbb{Q}$.
2. Correct according to *2.4.32* in the notes.

Exercice 2.
Considérons l'homomorphisme

$$\xi_p : \begin{array}{ccc} \mathbb{Z}[t] & \to & \mathbb{F}_p[t] \\ \sum_{i=0}^n a_i t^i & \mapsto & \sum_{i=0}^n [a_i] t^i \end{array}$$

qui envoie un polynôme à coefficients dans $\mathbb{Z}$ au polynôme obtenu par réduction des coefficients mod p. Soit $f(t)$ un polynôme dans $\mathbb{F}_p[t]$ et $g(t)$ une pré-image par ξ_p. Montrez que la pré-image de l'idéal $((f(t)))$ est $(p, g(t))$.

Solution. Nous allons procéder de deux manières différentes.

1. Non-explicite: Cet homomorphisme est surjectif de noyau (p). Comme la pré-image de $(f(t))$ et $(p, g(t))$ contiennent les deux (p), on sait par le théorème de correpondance qu'il suffit de montrer que leur image via $\mathbb{Z}[t] \to \mathbb{F}_p[t]$ sont les mêmes. Comme elles sont les deux $(f(t))$ par construction, on est bon.
2. Explicite: tout d'abord, vu que p et $g(t)$ sont dans $\xi_p^{-1}((f(t))$, alors automatiquement

   $$(p, g(t)) \subseteq \xi_p^{-1}((f(t)).$$

   Soit maintenant $h \in \xi_p^{-1}((f(t))$, et écrivons $\xi_p(h(t)) = \lambda(t) f(t)$, avec $\lambda(t) \in \mathbb{F}_p[t]$. Soit de plus $\mu(t)$ tel que $\xi_p(\mu(t)) = \lambda(t)$. Alors on obtient que

   $$\xi_p(\mu(t) g(t)) = \lambda(t) f(t) = \xi_p(h(t)),$$

   te donc que $\mu(t) g(t) - h(t) \in \ker(\xi_p) = (p)$. Ainsi, il exists $w(t)$ tel que

   $$h(t) = \mu(t) g(t) - p w(t) \in (p, g(t)),$$

   et donc on a bel et bien que

   $$\xi_p^{-1}((f(t))) \subseteq (p, g(t)).$$

Exercice 3.
Prouvez les affirmations suivantes.

1. Un anneau intègre avec un nombre fini d'éléments est un corps.
2. Soit K un corps et A un anneau commutatif.
   (a) Soit $K \to A$ un morphisme d'anneau. Montrez que multiplier par l'image des éléments de K fait de A un K-espace vectoriel avec son addition qui vient de la structure d'anneau de A.
   (b) Si maintenant A est intègre et de dimension finie en tant qu'espace vectoriel avec la structure ci-dessus, montrez que A est un corps.

Solution. Dans les deux cas on utilise l'argument suivant: la multiplication par un élément non-nul est injective (par intégrité), et donc dans nos cas surjective. Cette déduction est valide dans le premier cas car une fonction injective d'un ensemble fini vers lui même est injective si et seulement si surjective, et c'est aussi vrai pour les endomorphismes K-linéaires de K-espaces vectoriels de dimension finie.

Exercice 4.
Soit $f\colon A \to B$ un homomorphisme d'anneaux.

1. Montrer que $\mathrm{car}(B)$ divise $\mathrm{car}(A)$, mais qu'en général $\mathrm{car}(B) \neq \mathrm{car}(A)$.
2. Montrer que si f est injectif alors $\mathrm{car}(B) = \mathrm{car}(A)$.
3. Montrer que si A est commutatif et $\mathrm{car}(A) = p$, un nombre premier, alors l'application $F\colon A \to A$ définie par $F(a) = a^p$ est un homomorphisme d'anneaux.
4. Calculer la caractéristique de l'anneau $\mathbb{Z}[i]/(i-2)$.

Solution. Let $\iota_A : \mathbb{Z} \to A$ be the unique ring homomorphism with source $\mathbb{Z}$. By definition, $\mathrm{car}(A) = n$, where $\ker(\iota_A) = (n)$.

1. Consider the composition $\iota_B\colon \mathbb{Z} \xrightarrow{\iota_A} A \xrightarrow{f} B$. Since the kernel of the first homomorphism is contained in the kernel of the composition, it holds that $(n) = \ker(\iota_A) \subseteq \ker(\iota_B) =: (m)$, with m being $\mathrm{car}(B)$. Therefore, $m\big|n$, and so $\mathrm{car}(B)\big|\,\mathrm{car}(A)$.

   In general, $\mathrm{car}(B) \neq \mathrm{car}(A)$, as one can see when considering the reductions modulo 2, $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.
2. If f is injective, then its kernel is trivial, meaning that $\ker(\iota_A) = \ker(f \circ \iota_A) = \ker(\iota_B)$.
3. In order to show that F is a ring homomorphism, we show that $\forall a, b \in A$,
   - $F(1) = 1^p = 1$,
   - $F(ab) = (ab)^p = a^p b^p = F(a)F(b)$,
   - lastly, $F(a+b) = (a+b)^p = a^p + b^p$. This holds due to the fact that A is commutative, and the fact that the binomial coefficients that would appear for expressions of the form $a^i b^j$, $i, j \neq 0, i, j \neq p$ are all divisible by p, and hence they are zero in A.
4. Denote by g the unique homomorphism $g : \mathbb{Z} \to \mathbb{Z}[i]/(i-2)$. The characteristic of $\mathbb{Z}[i]/(i-2)$ is $k \in \mathbb{Z}$, where $(k) = \ker(g)$. The kernel is $\ker(g) = \{n \in \mathbb{Z}\big|\exists a, b \in \mathbb{Z} \text{ s.t } n = (a+ib)(i-2)\}$. Let $n \in \mathbb{Z}$ be contained in the kernel. Then, with $a, b \in \mathbb{Z}$,

$$n = (a+ib)(i-2) = (-2a-b) + i(a-2b).$$

   It follows that $n = -5b$, and so $n \in (5)$. Conversely, for $m \in (5)$, we have $m = 5\alpha$ for some $\alpha \in \mathbb{Z}$ and $g(m) = g(5\alpha) = g(5)g(\alpha) = 0$. This shows that $\ker(g) = (5)$.

Exercice 5.
Soit $A = \mathbb{Z}/250\mathbb{Z}$.

1. Trouver tous les diviseurs de zéro et tous les éléments inversibles de A.
2. Trouver tous les idéaux de A qui contiennent l'élément $[50]_{250}$. (Ce qu'on veut dire par cette notation c'est l'image de 50 dans $\mathbb{Z}/250\mathbb{Z}$.)

Solution. Let $A = \mathbb{Z}/250\mathbb{Z}$.

1. The zero divisors are the divisors of 250 and their multiples, stictly bigger than 1. The divisors of 250 (1 excluded) are $2, 5, 10, 25, 50, 125$ and 250.

   - For the divisor 2, we get 124 multiples, up to the last multiple 248.
   - For the divisor 5, we get 49 multiples, up to the last multiple 245. However, as half of these multiples are even, they have already been counted as multiples of 2. We get 25 new zero divisors.
   - The remaining divisors $10, 25, 50$ and 125 are multiples of 5 and have therefore already been counted into those zero divisors.

   Summing up, we get $124 + 25 = 149$ zero divisors.

   The remaining 100 elements are all invertible. Such an element $x \in A$ is prime to 250, meaning that x and 250 don't have any common divisors other than 1. With Bézout's identity there are two $a, b \in \mathbb{Z}$ such that $1 = ax + b \cdot 250$. With this, $ax \equiv 1 \bmod 250$.

2. By the correspondence theorem described in *Propositon 2.4.39*, the ideals of $A = \mathbb{Z}/250\mathbb{Z}$ correspond to ideals of $\mathbb{Z}$ which contain (250). Ideals of $\mathbb{Z}$ are principal, of the form (n). With $(250) \subseteq (n)$ we get that $n|250$ and so $n = 1, 2, 5, 10, 25, 50, 125$ and 250. Additionally, if the ideal in A contains 50, then the ideals in $\mathbb{Z}$ need to contain the preimage of the class [50]. In particular, they need to contain 50. Hence n is reduced to $1, 2, 5, 10, 25, 50$. The ideals in A are $A, ([2]), ([5]), ([10]), ([25])$ and $([50])$.

Exercice 6.
Soit A le sous-anneau de $M_2(\mathbb{Z})$ des matrices de la forme $\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}$ où $a, b, c \in \mathbb{Z}$. Montrez que le sous-ensemble K des matrices pour lesquelles $5 \mid a$ et $11 \mid b$ est un idéal bilatère et construire un isomorphisme (en deux temps) $A/K \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.

Solution. Soit A le sous-anneau de $M_2(\mathbb{Z})$ des matrices de la forme $\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}$ où $a, b, c \in \mathbb{Z}$. Montrer que le sous-ensemble K des matrices pour lesquelles $5 \mid a$ et $11 \mid b$ est un idéal bilatère et construire un isomorphisme (en deux temps) $A/K \to \mathbb{Z}/5 \times \mathbb{Z}/11$.

One verifies easily that the subset K is an additive subgroup, and that the product of a matrix in A and a matrix in K is a matrix in K, with multiplication in both directions. Therefore, K is a two-sided ideal.

To construct the isomorphism, we define the ideal I as

$$I := \left\{ \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} \middle| c \in \mathbb{Z} \right\}.$$

Again, verifying that this is an ideal is easy. Since $I \subset K$, we may apply the *Proposition 1.4.39 (Quotient en deux temps)*. Let $\xi : A \to A/I$. Then,

$$A/K \cong (A/I)/\xi(K).$$

We have that

$$\xi(K) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in \mathbb{Z}, 5 \mid a, 11 \mid b \right\}.$$

Furthermore, we note that A/I can be described as classes of matrices with representatives of the form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ with $a, b \in \mathbb{Z}$. This is isomorphic to $\mathbb{Z} \times \mathbb{Z}$ via the obvious isomorphism

$$\phi : \begin{array}{ccc} A/I & \to & \mathbb{Z} \times \mathbb{Z} \\ \left[\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right] & \mapsto & (a, b) \end{array}.$$

With ϕ, $\xi(K)$ is sent to $(5) \times (11)$, and therefore, $(A/I)/\xi(K) \cong (\mathbb{Z} \times \mathbb{Z})/((5) \times (11)) \cong \mathbb{Z}/(5) \times \mathbb{Z}/(11)$.

Exercice 7.
Soit R un anneau commutatif.

1. Montrer que $R[x, y]/(x) \cong R[y]$ (donner la forme explicite d'un isomorphisme).
2. Construire un homomorphisme d'anneaux $R[x, y] \to R[x] \times R[y]$ dont le noyau est (xy).
3. Identifier l'image de cet homomorphisme et en conclure que $R[x, y]/(xy)$ est isomorphe au sous-anneau de $R[x] \times R[y]$ formé des couples de polynômes $(p(x), q(y))$ tels que $p(0) = q(0)$.

Solution.

1. We use the universal property of polynomial rings, applied to the identity on $R[y]$. to obtain a ring homomorphism $ev_0 : R[y][x] \to R[y]$ s.t. $id_{R[y]} = \iota \circ ev_0$, where ι denotes the inclusion $\iota : R[y] \to R[y][x]$. ev_0 acts by sending a polynomial $p(x, y) \in R[y][x] \cong R[x, y]$ to $p(0, y) \in R[y]$. One easily verifies that ev_0 is surjective, as the identity on $R[y]$ is surjective. The kernel of ev_0 consists of all polynomials $p(x, y) \in R[x, y]$ for which $p(0, y) = 0$. These are exactly those polynomials that are multiples of x, and hence $\ker(ev_0) = (x)$. By the isomorphism theorem it follows that $R[y] \cong R[x, y]/(x)$.

2. As above, consider the two evaluations

$$ev_{0,x} := \begin{array}{ccc} R[x, y] & \to & R[y] \\ p(x, y) & \mapsto & p(0, y) \end{array}, \quad ev_{0,y} := \begin{array}{ccc} R[x, y] & \to & R[x] \\ p(x, y) & \mapsto & p(x, 0) \end{array}.$$

It holds that $\ker(ev_{0,y}) = (y)$. Using the universal property of products, we get a unique homomorphism

$$\phi : \begin{array}{ccc} R[x, y] & \to & R[x] \times R[y] \\ p(x, y) & \mapsto & (p(x, 0), p(0, y)) \end{array}.$$

The kernel of ϕ is equal to $\ker(ev_{0,x}) \cap \ker(ev_{0,y}) = (x) \cap (y) = (xy)$. Indeed, the inclusion

$$(xy) \subset (x) \cap (y)$$

holds immediately – as for the other inclusion, say $xf = yg$ for $f, g \in R[x, y]$ *i.e* an element of $(x) \cap (y)$. Note that $ev_{0,y}(xf) = xf(0, y) = 0$. As x is not a divisor of zero in $R[x]$, we conclude that $f(0, y) = 0$. Therefore $f \in (y)$, showing that $xf \in (xy)$.

3. We note that for a polynomial $p(x, y) \in R[x, y]$ the constant term of $ev_{0,x}(p)$ and of $ev_{0,y}(p)$ is the same. This suggests that the image of ϕ is as stated. To show that every such element is in the image of ϕ, we let $p(x) \in R[x]$ and $q(y) \in R[y]$. Consider the pair $(a + xp(x), a + yq(y)) \in R[x] \times R[y]$ with $a \in R$. Then

$$\phi(a + xp(x) + yq(y)) = (a + xp(x), a + yq(y)).$$

Therefore, the pair $(a + xp_x(x), a + yp_y(y))$ is contained in the image of ϕ. We conclude with the isomorphism theorem.