EPFL - Printemps 2024 Prof. Zs. Patakfalvi
Anneaux et Corps **Exercices**
Solutions 3

Exercice 1. 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 *Lemma 1.4.30.*

Exercice 2.
Assume that $\xi_p^{-1}(I)$ is principal, meaning that $\xi_p^{-1}(I) = (f)$ for some $f \in \mathbb{Z}[t]$. Since I is by definition an additive group, it contains 0, and therefore $p \in \xi_p^{-1}(I) = \mathbb{Z}[t] \cdot f$. It follows that $p = g \cdot f$ for some $g \in \mathbb{Z}[t]$. We recall that by Exercise 5 on Sheet 2, $\deg(f \cdot g) = \deg(f) + \deg(g)$. It follows that

$$0 = \deg(p) = \deg(f \cdot g) = \deg(f) + \deg(g).$$

Therefore, $\deg(f) = 0$ and $\deg(g) = 0$ and so $f, g \in \mathbb{Z}$. But then $p = g \cdot f$. Since p is prime, it follows that either $f = \pm 1$ or $f = \pm p$. If $f = \pm 1$, then $I = \mathbb{F}_p[t]$. If $f = \pm p$, then $I = \{0\}$. Those are contradictions to the assumption and therefore, $\xi_p^{-1}(I)$ is not principal.

Exercice 3. 1. **Identité de Bézout.** Let d be the biggest common divisor of m and n. Define the set $E := \{cm + dn \big| c, d \in \mathbb{Z}\}$. Let $e = am + bn$ be the smallest non-zero positive integer in E. Dividing n by e with rest, we get $n = qe + r$ for some $q \in \mathbb{Z}, 0 \leq r < e$. Then

$$r = n - qe = n - q(am + bn) = \underbrace{(-qa)}_{\in\mathbb{Z}} m + \underbrace{(1 - qb)}_{\in\mathbb{Z}} n \in E.$$

But since $r < e$, it follows that $r = 0$, and therefore $e \big| n$. Similarly, we show that $e \big| m$. It follows that e is a common divisor of m and n. It remains to show that e is indeed the biggest common divisor. Since $d \big| m$ and $d \big| n$, it holds that $d \big| (am + bn) = e$, and hence $e = d$.

2. We have

- $(m)(n) = (mn)$ by *Remarque 1.4.28.*
- $(m) + (n) = (m, n)$ by *Remarque 1.4.28.* According to Bézout, this is equal to (d).
- $(m) \cap (n) = (\text{ppmc}\{m, n\})$. The inclusion $\supseteq$ holds due the definition, which states that $(m) \cap (n)$ contains elements that are simultaneously in (m) and (n), which means that they are simultaneously multiples of (m) and of (n). For the other inclusion, let k be an element contained in $(m) \cap (n)$. That means that k is a multiple of both (m) and (n). Let p be the least common multiple of m and n. As in the first part of this exercise, we can divide k by p with rest, from which it follows that k is a multiple of p, and therefore $k \in (\text{ppmc}\{m, n\})$.

Exercice 4.
Let $\iota_A : \mathbb{Z} \to A$ be the unique ring homomorphism with source $\mathbb{Z}$. By definition, $\text{car}(A) = n$, 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 $\operatorname{car}(B)$. Therefore, $m \big| n$, and so $\operatorname{car}(B) \big| \operatorname{car}(A)$.

   In general, $\operatorname{car}(B) \neq \operatorname{car}(A)$, 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.
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 described in *Propositon 1.4.36*, 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 $n \big| 250$ 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 $a, b, c \in \mathbb{Z}$. 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.

1. We use *Proposition 1.2.2.* applied to the identity on $R[y]$. The proposition then states that there exists a unique 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, *Proposition 1.4.45*, 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.