Leonid Monin
Léo Navarro Chafloque

Exercices – Semaine 3

Exercice 1.
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 $\mathbb{Z}[i]/(i-2)$. À quoi cet anneau est-il isomorphe ?
5. Même questions pour $\mathbb{Z}[i]/(i+3)$.

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 $\ker(g) = (5)$.

   On montre maintenant que le morphisme g est surjectif. Il suffit que l'image de i soit atteinte. Mais $i = 2$ dans l'anneau quotient, ce qui conclut. Maintenant, on utilise le théorème d'isomorphisme pour avoir

   $$\mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}[i]/(i-2)$$

5. On utilise que
$$\mathbb{Z}[i] \cong \mathbb{Z}[t]/(t^2+1).$$
En effet, il suffit de montrer que le noyau de l'évaluation en i de $\mathbb{Z}[t] \to \mathbb{Z}[i]$ est (t^2+1). Cela se déduit par division euclidienne et en utilisant que $i \notin \mathbb{Z}$.

Maintenant le quotient $\mathbb{Z}[i]/(i+3)$ s'identifie en utlisant l'isomorphisme ci-dessus a
$$\mathbb{Z}[t]/(t+3, t^2+1).$$
On quotiente une première fois par $(t+3)$ en utilisant l'évaluation $\mathbb{Z}[t] \to \mathbb{Z}$ en -3 pour obtenir que le quotient ci-dessus s'identifie à
$$\mathbb{Z}/((-3)^2+1) = \mathbb{Z}/(10).$$

Exercice 2.
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 $n \big| 250$ 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 3.
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 quotient in two times, first by I and then by K. 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 4.
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.

Exercice 5.
Dans chacun des cas suivants, déterminer si l'idéal proposé est premier ou maximal.

(a) $(0) \subset \mathbb{Z}$.
(b) $(t) \subset \mathbb{Z}[t]$.
(c) $(t) \subset \mathbb{R}[t]$.
(d) $(101) \subset \mathbb{Z}[t]$.
(e) $(42) \subset \mathbb{Z}[t]$.
(f) $(t^2 - 2) \subset \mathbb{Z}[t]$.
(g) $(t^2 - 2) \subset \mathbb{R}[t]$.
(h) $(t + 5, 10) \subset \mathbb{Z}[t]$.
(i) $(t + 5, 11) \subset \mathbb{Z}[t]$.
(j) $(t^2 + 1, 2) \subset \mathbb{Z}[t]$.

Indication : Pour prouver qu'un idéal bilatère $I \subset A$ est premier, il suffit de montrer que le quotient A/I est intègre.

Solution.

1. $(0) \subset \mathbb{Z}$ est premier car $\mathbb{Z}$ est intègre, non maximal car $(0) \subsetneq (2)$.
2. $(t) \subset \mathbb{Z}[t]$ est premier car le quotient $\mathbb{Z}$ est intègre, non maximal car $(t) \subsetneq (t, 2) \neq \mathbb{Z}[t]$.
3. $(t) \subset \mathbb{R}[t]$ est premier et maximal car le quotient est un corps.
4. $(101) \subset \mathbb{Z}[t]$ est premier. En effet, considérons l'homomorphisme

$$\xi \colon \mathbb{Z}[t] \longrightarrow (\mathbb{Z}/101\mathbb{Z})[t], \quad \sum_i a_i t^i \mapsto \sum_i [a_i]_{101} t^i.$$

Il est clair que $f(t) = \sum_i a_i t^i \in \ker \xi$ si et seulement si $[a_i]_{101} = 0$ pour chaque i, donc si et seulement si 101 divise chaque coefficient, donc si et seulement 101 divise $f(t)$. Cela prouve que $\ker \xi = (101)$. Pour conclure, il suffit de montrer que $(\mathbb{Z}/101\mathbb{Z})[t]$ est un anneau intègre. Puisque 101 est un nombre premier, $\mathbb{Z}/101\mathbb{Z}$ est un anneau intègre. De manière générale, si A est un anneau intègre alors $A[t]$ est aussi intègre (la preuve est un bon exercice), ce qui conclut.

5. $(42) \subset \mathbb{Z}[t]$ n'est pas premier car $6 \cdot 7 = 42$, donc non maximal.

6. $(t^2-2) \subset \mathbb{Z}[t]$ est premier. En effet, considérons l'homomorphisme d'évaluation

$$\mathrm{ev}_{\sqrt{2}} \colon \mathbb{Z}[t] \longrightarrow \mathbb{R}, \quad t \mapsto \sqrt{2}.$$

On montre comme dans l'Exemple 2.4.19 que $\ker \mathrm{ev}_{\sqrt{2}} = (t^2-2)$. Comme $\mathbb{Z}[t]/(t^2-2)$ est isomorphe à un sous-anneau de $\mathbb{R}$, c'est un anneau intègre, et donc (t^2-2) est premier.

Ce n'est pas un ideal maximal, puisque $(t^2-2) \subsetneq (t^2-2,3) \neq \mathbb{Z}[t]$. Alternativement, on peut vérifier que $\mathrm{im}\, \mathrm{ev}_{\sqrt{2}} = \mathbb{Z}[\sqrt{2}]$ n'est pas un corps (par exemple 3 n'a pas d'inverse).

7. $(t^2-2) \subset \mathbb{R}[t]$ n'est pas premier car $t^2-2 = (t-\sqrt{2})(t+\sqrt{2})$ dans $\mathbb{R}[t]$.

8. $(t+5, 10) \subset \mathbb{Z}[t]$ n'est pas premier car $10 = 2 \cdot 5$.

9. $(t+5, 11) \subset \mathbb{Z}[t]$ est maximal (donc premier) car le quotient est le corps $\mathbb{Z}/11\mathbb{Z}$.

10. $(t^2+1, 2) \subset \mathbb{Z}[t]$ n'est pas premier car $(t+1)^2 = t^2+1+2t \in (t^2+1, 2)$.

Exercice 6.
Soient A et B deux anneaux commutatifs. Quels sont les idéaux de $A \times B$? Quels sont les idéaux premiers de $A \times B$?

Solution. Soit $J \leq A \times B$ un idéal. Noter que $(0,1)J \leq \{0\} \times B$ et $(1,0)J \leq A \times \{0\}$ sont des idéaux de $A \times B$ inclus dans J. De plus, noter que $J = (1,0)J \times (0,1)J$. On conclut donc que tout idéal du produit est de la forme $I_A \times I_B$ pour I_A et I_B des idéaux quelconques de A et B respectivement.

En ce qui est des idéaux premiers, on voit en utilisant qu'un idéal est premier si et seulement si le quotient par cet idéal est intègre que les idéaux premiers sont de la forme

$$\mathfrak{p}_A \times B \quad A \times \mathfrak{p}_B$$

pour $\mathfrak{p}_A$ et $\mathfrak{p}_B$ des idéaux premiers de A et B respectivement.

Exercice 7.
Soit A un anneau commutatif.

1. Montrez que si $\mathfrak{m}$ est maximal et est composé uniquement d'éléments nilpotents, alors c'est l'unique idéal maximal de A. La réciproque est-elle vraie ?

2. Montrez que $A \setminus A^\times$ est un idéal si et seulement si A a un unique idéal maximal.

Solution.

1. Notons que $\mathfrak{m} \subset \mathrm{nil}(A)$ par hypothèse implique en fait $\mathfrak{m} = \mathrm{nil}(A)$ par maximalité. Maintenant si $\mathfrak{m}'$ est un autre idéal maximal, on a $\mathrm{nil}(A) \subset \mathfrak{m}'$ Mais alors on a encore égalité par maximalité, ce qui conclut. La réciproque est fausse, considérez $\mathbb{Z}_{(p)}$ (c.f. l'exercice 1 de la série 1.2).

2. Notons que tout idéal propre est contenu dans $A \setminus A^\times$. En effet si un élément inversible appartient à un idéal, celui-ci est forcément égal à A. Dès lors si $\mathfrak{m}$ est maximal (en particulier propre), on a $\mathfrak{m} \subset A \setminus A^\times$. Mais comme on a supposé que $A \setminus A^\times$ est un idéal, on a par maximalité $\mathfrak{m} = A \setminus A^\times$.

   Réciproquement si A a un unique idéal maximal $\mathfrak{m}$, alors $A \setminus \mathfrak{m} = A^\times$. En effet $\supset$ suit, sinon il y a un élément inversible dans $\mathfrak{m}$, ce qui contredirait le caractère propre de $\mathfrak{m}$. Pour l'autre inclusion prenons $x \in A \setminus \mathfrak{m}$. Par l'absurde supposons que x ne soit pas inversible. Alors (x) est un idéal propre est donc inclus dans un idéal maximal. Mais par hypothèse on a alors $(x) \subset \mathfrak{m}$ ce qui est absurde.

Remarque. Une des clés pour l'exercice ci-dessus qui peut-être non évidente à première vue mais qui est fondamentale est que les éléments nilpotents appartiennent à tous les idéaux premiers d'un anneau commutatifs. En effet soit $\mathfrak{p}$ un idéal premier d'un anneau commutatif A et $x \in A$ un élément nilpotent. Si $x^n = 0$ alors comme $0 \in \mathfrak{p}$ on a en utilisant la primalité que $x \in \mathfrak{p}$.

Exercice 8.
Soit

$$\mathbb{H} := \mathbb{R} \oplus i\mathbb{R} \oplus j\mathbb{R} \oplus k\mathbb{R}$$

l'anneau non-commutatif des *quaternions*. La multiplication est inférée des relations suivantes:

$$k = ij \quad i^2 = j^2 = k^2 = -1 \quad ij = -ji$$

Montrez que tout élément non-nul de $\mathbb{H}$ a un inverse multiplicatif. (Pensez à l'inverse dans le cas complexe.)

Solution. Soit $x = a + ib + jc + kd \in \mathbb{H}$. On définit $\overline{x} := a - ib - jb - kc$. Notons que cela définit une application $\mathbb{R}$-linéaire sur $\mathbb{H}$ d'ordre 2. On définit $N(x) = a^2 + b^2 + c^2 + d^2$. Parce que les réels $\mathbb{R} \subset \mathbb{H}$ commutent avec tous les éléments on a

$$x\overline{x} = a^2 - (ib + jb + kc)^2.$$

En utlisant que $ij = -ji$, $ik = -ki$, $jk = -kj$ et que $i^2 = j^2 = k^2 = -1$ on obtient que $-(ib + jb + kc)^2 = b^2 + c^2 + d^2$. Ainsi $x\overline{x} = N(x)$. En appliquant $\overline{(-)}$ à cette égalité on obtient également $N(x) = \overline{x}x$. Donc si x est non-nul on déduit que $x \cdot \frac{\overline{x}}{N(x)} = 1 = \frac{\overline{x}}{N(x)} \cdot x$.