EPFL - Printemps 2025 | Prof. Zs. Patakfalvi
**Anneaux et Corps** | **Exercices**
Solutions 3

**Exercice 1.** 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 2.** 1. Le premier système n'a pas de solutions. En effet, si $x = 7 + 12k$, alors $x = 1 + 3 \cdot (2 + 4k)$, ce qui contredit $x \equiv 2 \pmod 3$.
Le second système admet une infinité de solutions. En effet, si $x = 8 + 12k$, alors $x = 2 + 3 \cdot (2 + 4k)$. Donc le système est équivalent à $x \equiv 8 \pmod{12}$, qui admet une infinité de solutions.

2. Pour voir que $\mathbb{Z}/36\mathbb{Z} \ncong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ on peut par exemple utiliser le fait que le deuxième anneau n'est pas cyclique en tant que groupe abélien : tout élément est d'ordre un diviseur de 12.

**Exercice 3.** 1. Prenons $x \in f^{-1}(I)$. Alors $f(x) \in I$ et, par définition de $I$, on peut écrire

$$f(x) = \sum_{i=1}^{n} \beta_i b_i, \quad \text{pour certains } \beta_i \in B.$$

Puisque $f$ est surjective, on peut choisir des $\alpha_i \in A$ tels que $f(\alpha_i) = \beta_i$. Posons

$$x' := \sum_{i=1}^{n} \alpha_i c_i.$$

Par construction $f(x) = f(x')$, et donc $x - x' \in \ker f$. Ainsi il existe des $\gamma_i \in A$ tels que

$$x - x' = \sum_{i=1}^{m} \gamma_i a_i$$

et cette égalité se réarrange en

$$x = \sum_{i=1}^{m} \gamma_i a_i + \sum_{i=1}^{n} \alpha_i c_i \in (a_1, \ldots, a_m, c_1, \ldots, c_n).$$

Comme $x$ est arbitraire, cela montre que $f^{-1}(I) \subseteq (a_1, \ldots, a_m, c_1, \ldots, c_n)$. L'inclusion inverse est immédiate, puisque

$$f(a_i), f(c_j) \in I \quad \forall i, j.$$

On a donc démontré l'égalité désirée.

2. L'Exercice 6.a) de la série 1.2 montre que $\ker \mathrm{ev}_b = (y - b)$ et $\ker \mathrm{ev}_a = (x - a)$. Puisque $\ker \xi = \mathrm{ev}_b^{-1}(\ker \mathrm{ev}_a)$ (l'égalité est facile à vérifier), par le point précédent on obtient que $\ker \xi = (x - a, y - b)$.
   Puisque $\xi(\lambda) = \lambda$ pour tout $\lambda \in k$, on voit que $\xi$ est surjective. Par le premier théorème d'isomorphisme, on obtient $k \cong k[x, y]/\ker \xi$. Par la Proposition 2.5.5, on obtient que $\ker \xi$ est un idéal maximal.

**Exercice 4.**
**Nota bene :** la discussion des deux derniers points de cet exercice pourra être grandement simplifiée une fois à disposition les propriétés des polynômes irréductibles.

1. On sait par l'Exemple 2.4.19 que le morphisme $\mathbb{Z}[x] \to \mathbb{Z}[i]$ donné par l'évaluation en $i$ induit un isomorphisme $\theta\colon \mathbb{Z}[x]/(x^2 + 1) \to \mathbb{Z}[i]$. De plus, $p + (x^2 + 1)$ est envoyé sur $p$ par cet isomorphisme, et donc on en déduit un isomorphisme

$$(\mathbb{Z}[x]/(x^2 + 1))/(p + (x^2 + 1)) \cong \mathbb{Z}[i]/(p).$$

   Par le théorème du quotient en deux temps appliqué deux fois, on a que

$$(\mathbb{Z}[x]/(x^2 + 1))/(p + (x^2 + 1)) \cong \mathbb{Z}[x]/(p, x^2 + 1) \cong (\mathbb{Z}[x]/(p))/(x^2 + 1 + (p)).$$

   De plus, il est immédiat que le morphisme $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ induit par la réduction modulo $p$ et envoyant $x$ sur $x$ est surjectif, de noyau $(p) \subseteq \mathbb{Z}[x]$. Il induit donc un isomorphisme $\mathbb{Z}[x]/(p) \cong \mathbb{F}_p[x]$. Comme ce morphisme envoit $x^2 + 1 + (p)$ sur $x^2 + 1$, on a donc un isomorphisme induit

$$\mathbb{Z}[x]/(p, x^2 + 1) \cong (\mathbb{Z}[x]/(p))/(x^2 + 1 + (p)) \cong \mathbb{F}_p[x]/(x^2 + 1).$$

2. Dans le cas où $p = 5$, on remarque que $[2]_5$ et $[3]_5$ sont des racines de $t^2 + [1]_5 \in \mathbb{F}_5[t]$. En particulier on a la factorisation

$$t^2 + [1]_5 = (t - [2]_5) \cdot (t - [3]_5). \tag{1}$$

   Remarquez que $(t - [2]_5) - (t - [3]_5) = [1]_p$. Donc les idéaux générés respectivement par $t - [2]_5$ et par $t - [3]_5$ sont premiers entre eux. Le théorème des restes chinois donne alors

$$\frac{\mathbb{F}_5[t]}{(t - [2]_5) \cap (t - [3]_5)} \cong \frac{\mathbb{F}_5[t]}{(t - [2]_5)} \times \frac{\mathbb{F}_5[t]}{(t - [3]_5)}. \tag{2}$$

   L'évaluation en $t = [2]_5$ induit un ismorphisme

$$\mathbb{F}_5 \cong \frac{\mathbb{F}_5[t]}{(t - [2]_5)}$$

et d'une manière similaire on a

$$\mathbb{F}_5 \cong \frac{\mathbb{F}_5[t]}{(t-[3]_5)}.$$

On prétend pour finir que $(t-[2]_5) \cap (t-[3]_5) = (t^2+[1]_5)$. L'inclusion $\supseteq$ est claire, en vue de la factorisation (1). Inversément, prenons un élément $f(t)$ appartenant à l'intersection des deux idéaux. On peut écrire

$$(t-[2])g(t) = f(t) = (t-[3])h(t)$$

pour certains $g(t), h(t) \in \mathbb{F}_5[t]$. Considérons l'image de $f(t)$ par l'évaluation $\mathrm{ev}_{[2]}$ en $t=[2]$. On a

$$\mathrm{ev}_{[2]}(f(t)) = \mathrm{ev}_{[2]}((t-[2])g(t)) = 0$$

d'une part, et

$$\mathrm{ev}_{[2]}(f(t)) = \mathrm{ev}_{[2]}((t-[3])h(t)) = -\mathrm{ev}_{[2]}(h(t))$$

d'autre part. Ainsi $\mathrm{ev}_{[2]}(h(t)) = 0$, et puisque $\ker \mathrm{ev}_{[2]} = (t-[2])$ on en déduit que $h(t) = (t-[2])j(t)$ pour un certain $j(t) \in \mathbb{F}_5[t]$. On peut ainsi écrire

$$f(t) = (t-[3])(t-[2])j(t) = (t^2+[1])j(t)$$

ce qui montre que $f(t) \in (t^2+[1])$.
En combinant tout cela dans (2), on obtient

$$\frac{\mathbb{F}_5[t]}{(t^2+[1])} \cong \mathbb{F}_5 \times \mathbb{F}_5,$$

ce qui implique que $\mathbb{Z}[i]/(5) \cong \mathbb{F}_5 \times \mathbb{F}_5$ en vue du point précédent.

3. Montrons tout d'abord que 4 divise $p-1$ (i.e. $p \equiv 1 \mod 4$) si et seulement si $-1$ possède deux racines distinctes modulo $p$.
Tout d'abord, aucun des deux côtés de l'équivalence n'est satisfait si $p=2$, donc supposons que $p \neq 2$. Dans ce cas, il suffit de montrer que 4 divise $p-1$ si et seulement si $-1$ est un carré modulo $p$ (si $a \in \mathbb{F}_p$ satisfait $a^2 = -1$, alors $-a$ aussi et vu que $p \neq 2$, il y a automatiquement deux racines carrés de $-1$).

Supposons tout d'abord qu' il existe $a \in \mathbb{F}_p$ tel que $a^2 = -1$. Vu que $p \neq 2$, $a$ est donc un élément d'ordre 4 dans le groupe multiplicatif $(\mathbb{F}_p^\times, \cdot)$, qui est d'ordre $p-1$. Ainsi, 4 divise $p-1$ par le théorème de Lagrange.
Si 4 divise $p-1$, alors vu que l'on sait par le cours que l'on a un isomorphisme de groupes $(\mathbb{F}_p^\times, \times) \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +)$, et que dans $\mathbb{Z}/(p-1)\mathbb{Z}$, l'élément $\frac{p-1}{4}$ est d'ordre 4, on obtient l'existence d'un élément $a$ d'ordre 4 dans $(\mathbb{F}_p^\times, \times)$.

Montrons maintenant que $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p \times \mathbb{F}_p$ si et seulement si $-1$ a une racine carrés (encore une fois, on exclut $p=2$ car $\mathbb{Z}[i]/(2) \cong \mathbb{F}_2/(x+1)^2$ qui ne peut pas être isomorphe à $\mathbb{F}_2 \times \mathbb{F}_2$, vu que l'un contient un élément nilpotent et que l'autre non).
Supposons d'abord que l'on puisse écrire $a^2 = [-1]_p = b^2$ dans $\mathbb{F}_p$ avec $a \neq b$. Puisque $\ker \mathrm{ev}_a = (t-a)$, on peut écrire

$$t^2 + [1]_p = (t-a)(t-b')$$

et on prétend que $b' = b$. En effet,

$$\mathbb{F}_p \ni 0 = b^2 + [1] = \mathrm{ev}_b(t^2+[1]) = \underbrace{(b-a)}_{\neq 0}(b-b')$$

et comme $\mathbb{F}_p$ est intègre, on obtient que $b - b' = 0$. De plus, $(t-a) - (t-b) = b - a \neq 0$ est un élément inversible de $\mathbb{F}_p$, donc les idéaux $(t-a)$ et $(t-b)$ sont premiers entre eux. En appliquant le théorème des restes chinois comme dans la partie précédente, on trouve que

$$\frac{\mathbb{F}_p[t]}{(t-a)\cap(t-b)} \cong \mathbb{F}_p \times \mathbb{F}_p.$$

Puisque $b - a \neq 0$ est inversible dans $\mathbb{F}_p$, on obtient comme dans le point précédent que $(t-a)\cap(t-b) = (t^2+[1])$ (où l'on avait utilisé que $[2]_5 - [3]_5 = -[1]_5$ est inversible dans $\mathbb{F}_5$), et donc que

$$\mathbb{Z}[i]/(p) \cong \frac{\mathbb{F}_p[t]}{(t^2+[1])} \cong \mathbb{F}_p \times \mathbb{F}_p.$$

Remarquons si $a \in \mathbb{F}_p$ est une racine carrée de $[-1]_p$, alors $-a$ en est aussi une. Or, vu que $p \neq 2$ on a $a \neq -a$. Il nous reste ainsi à traiter le cas où $-1$ n'a pas de racine carré modulo $p$. Pour finir, supposons qu'il n'existe pas de racine carrée de $-1$ dans $\mathbb{F}_p$. On prétend que $\mathbb{F}_p[t]/(t^2+[1])$ est un anneau intègre. Fixons une clotûre algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$, et choisissons une racine carrée $i \in \overline{\mathbb{F}_p}$ de $-1$. On considère l'homomorphisme d'évaluation

$$\mathrm{ev}_i \colon \mathbb{F}_p[t] \longrightarrow \overline{\mathbb{F}_p}, \quad t \mapsto i.$$

Puisque $\mathbb{F}_p[t]/\ker \mathrm{ev}_i \cong \mathrm{im}\, \mathrm{ev}_i \subset \overline{\mathbb{F}_p}$ et que $\overline{\mathbb{F}_p}$ est intègre, on voit que $\mathbb{F}_p[t]/\ker \mathrm{ev}_i$ est un anneau intègre. On prétend que $\ker \mathrm{ev}_i = (t^2+[1]_p)$. L'argument est le similaire à celui de l'Exemple 2.4.19. Pour finir, on prétend que $\mathbb{F}_p[t]/(t^2+[1])$ n'est pas isomorphe à $\mathbb{F}_p \times \mathbb{F}_p$ : en effet, cet anneau produit n'est pas intègre.

**Exercice 5.**
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 6.**

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 $\mathbb{Z}_{(p)}$.
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.

**Exercice 7.**
On suppose d'abord que $R$ est intègre. Grâce à la formule du degré, on voit que $R[t]^\times = R^\times$, donc les inversibles de $R$ en degré zéro.

On traite maintenant le cas général. Soit $\mathfrak{p}$ in idéal premier de $R$. Soit $f(t)$ un élément inversible. L'image dans $(R/\mathfrak{p})[t]$ est encore inversible. Ainsi, par le cas intègre, on voit que les coefficients

en degré strictement positif de $f(t)$ sont dans l'idéal $\mathfrak{p}$ et le terme constant n'est pas dans l'idéal. Ainsi, comme $\mathfrak{p}$ est quelconque,*

$$R[t]^\times \subseteq t\,\mathrm{nil}(R)[t] + R^\times.$$

L'inclusion inverse est également vérifiée. En effet, si $f(t) \in t\,\mathrm{nil}(R)[t] + R^\times$, alors $f(t) - a_0$ est nilpotent car c'est une somme d'éléments nilpotents. On conclut par 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,

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

∗. Un élément dans l'intersection de tout les premiers est nilpotent. Un élément dans aucun idéal maximal est inversible. Notons également que pour voir que le terme constant de $f(t)$ est inversible on peut évaluer en zéro.