Leonid Monin
Léo Navarro Chafloque

EPFL, semestre de printemps 2026
Rings and fields

Solutions – Semaine 5

Exercice 1.
Soit A un anneau commutatif. Soit k un corps. On dit qu'un élément $a \in A$ est *idempotent* si $a^2 = a$.

1. Quels sont les idempotents de $k \times k$?
2. Montrez que $e \in A$ est un idempotent si et seulement si $1 - e$ l'est aussi.
3. Soit e un idempotent de A. Montrez que l'application naturelle
$$A \to A/(e) \times A/(1-e)A$$
qui envoie $a \mapsto (\pi_e(a), \pi_{1-e}(a))$ où $\pi_e \colon A \to A/(e)$ et $\pi_{1-e} \colon A \to A/(1-e)$ sont les applications quotients est un isomorphisme.
4. Soit $n \in \mathbb{N}$. Déterminer tous les idempotents de
$$k[t]/(t^n).$$
Cet anneau est-il isomorphe à un produit d'anneau non-nuls ?

Solution.
Notons en premier lieu que les seuls idempotents d'un anneau intègre sont 0 et 1. En effet si
$$x^2 = x$$
alors
$$x(x-1) = 0.$$
Dans un anneau intègre on conclut que $x = 0, 1$.

1. Il faut que chaque composante soit un idempotent donc on voit qu'on a $(0,1), (1,0), (0,0) = 0, (1,1) = 1$.
2. Si e est idempotent alors $(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$. Cela suffit.
3. Montrons que les hypothèses du théorème chinois des restes s'applique. Premièrement $1 \in (e) + (1-e)$. Aussi, si $\alpha \in (e) \cap (1-e)$ alors $\alpha = ex = (1-e)y$. Donc $e\alpha = e^2x = ex = e(1-e)y = 0$. Cela conclut.
4. Notons que l'image d'un idempotent par un morphisme d'anneau est encore un idempotent. Tout élément de $k[t]/(t^n)$ est de la forme une classe
$$\sum_{i=0}^{n-1} a_i t^t.$$
Donc tout élément $x \in k[t]/(t^n)$ est de la forme $x = \lambda + \epsilon$ avec $\lambda \in k$ le terme constant du polynôme et ϵ nilpotent car t est nilpotent.* En effet la somme d'éléments nilpotents est encore nilpotente, ce qu'on voit grâce à la formule du binôme. En effet si a, b sont respectivement

*Dans un anneau A on dit que $a \in A$ est nilpotent s'il existe $n \in \mathbb{N}$ avec $a^n = 0$.

nilpotents avec $a^k = 0$ et $a^l = 0$ respectivement alors $(a+n)^{2m+1} = 0$ si $m = max(k,l)$ en dévellopant avec la formule du binôme.

On a le morphisme de réduction modulo t

$$k[t]/(t^n) \to k$$

qui envoie $\lambda + \epsilon \mapsto \lambda$. Dès lors si on suppose que $x = \lambda + \epsilon$ est un idempotent, on voit que $\lambda = 0, 1$. Traitons les deux cas. Si $\lambda = 0$ alors $x = \epsilon$ est idempotent est nilpotent, disons qu'on a $N \in \mathbb{N}$ avec $0 = \epsilon^N = \epsilon$. Maintenant le cas où $\lambda = 1$. Alors $1 - x = 1 - (1 - \epsilon) = \epsilon$ est aussi idempotent, et donc $\epsilon = 0$. Ainsi les seuls idempotents sont $0, 1$.

On voit donc que cet anneau ne peut-être isomorphe à un produit d'anneau non-nuls: un tel produit contient toujours au moins quatres idempotents distincts comme au premier point.

Exercice 2.
Déterminez quel idéaux sont premiers et ou maximaux dans les cas suivants.

1. $(3, t^3 + 1) \subset \mathbb{Z}[t]$.
2. $(t^3 + t + 1) \subset \mathbb{Z}[t]$.
3. $(3, t^3 + t + 1) \subset \mathbb{Z}[t]$.

Solution.

Notons que le théorème de correspondance se précise de la façon suivante pour les idéaux premiers

$$\{I \subset \mathfrak{p} \subset A \mid \mathfrak{p} \text{ premier}\} \leftrightarrow \{\mathfrak{q} \subset A/I \mid \mathfrak{q} \text{ premier}\}$$

qui envoie $\mathfrak{p}$ sur $\mathfrak{q} = \mathfrak{p}/I$. On voit cela car $A/\mathfrak{p} \cong (A/I)/\mathfrak{q}$ par le quotient en deux temps. On rappelle que les idéaux premiers sont exactement les idéaux dont le quotient est intègre.

On peut alors répondre aux questions 1. et 3 en quotientant par 3 d'abord. On cherche donc à determiner si dans $\mathbb{Z}/3\mathbb{Z}[t]$ les idéaux $(t^3 + 1)$ et $(t^3 + t + 1)$ sont premiers. Pour cela on remarque que

$$t^3 + 1 = (t+1)(t^2 - t + 1) \quad t^3 + t + 1 = (t-1)(t^2 + t - 1)$$

où la deuxième égalité utilise $-2 = 1$, valide dans $\mathbb{Z}/3\mathbb{Z}$. Maitenant $t - 1$ et $t + 1$ sont de degré 1 - s'ils étaient inclus dans les idéaux (t^3+1) et (t^3+t+1) respectivement on aurait une contradiction sur le degré car un polynôme de degré 3 ne peut diviser un polynôme de degré 1.

Quant au point 2. on affirme que cet idéal est premier. On fait un peu d'analyse en premier lieu. On considère la fonction $\mathbb{R} \to \mathbb{R}$ qui envoie $x \mapsto x^3 + x + 1$. Cette fonction est dérivable étant polynomniale et sa dérivée est donnée par $x \mapsto 3x^2 + 1$. Celle-ci est strictement positive. Dès lors comme la fonction est cubique, on voit que cette fonction s'annule en un unique point à l'ordre 1 (une racine double impliquerait que la dérivée s'annulerait aussi en α mais celle-ci est strictement positive) qu'on note $\alpha \in \mathbb{R}$.

Remarquons maintenant deux choses.

1. $\alpha \notin \mathbb{Q}$. Supposons que ce soit le cas, et prenons $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus 0$ premiers entre eux avec $\alpha = \frac{a}{b}$. Alors
$$\frac{a^3}{b^3} + \frac{a}{b} + 1 = 0.$$
Et donc
$$a(a^2 + b^2) = a^3 + ab^2 = -b^3.$$
Mais comme a, b n'ont aucun facteur premier en commun on voit que $a = \pm 1$. Alors on a
$$b^3 + b^2 + 1 = 0 \quad \text{ou} \quad b^3 + b^2 - 1 = 0.$$
En réduisant modulo 2 en obtient $0 = 2b + 1 = 1$, dans les deux cas, une contradiction.

2. Il ne peut y avoir de polynôme $g \in \mathbb{Q}[t]$ de degré 2 ou 1 qui annule α. En effet, dans le cas degré 1 on obtiendrait que $\alpha \in \mathbb{Q}$. Dans le cas de degré 2, si c'est le cas en divisant t^3+t+1 par g dans $\mathbb{Q}[t]$ on obtiendrait un reste de degré 1 ou zéro. Dans le cas où le reste est de degré 1 on obtiendrait un polynôme de degré 1 qui annule α et on revient au cas précédent, ce qui permet d'exclure ce cas. Dans l'autre cas on aurait dans $\mathbb{Q}[t]$ que t^3+t+1 est produit d'un polynôme de degré 2 et d'un polynôme de degré 1. Mais alors grâce au polynône de degré 1, on aurait un élément $q \in \mathbb{Q}$ qui satisferait $q^3+q+1=0$ ce qui est exclu par les arguments du premier point.

Fort de ces raisonnements, on affirme maintenant que le noyau de

$$\mathbb{Z}[t] \xrightarrow{\mathrm{ev}_\alpha} \mathbb{R}$$

est (t^3+t+1). Pour cela, on prend $f(t)$ dans le noyau est on mène la division euclidienne de $f(t)$ par t^3+t+1. Comme on a vu qu'il n'est pas possible qu'un polynôme de degré 1 ou de degré 2 à coefficients dans $\mathbb{Q}$, et a fortiori dans $\mathbb{Z}$, annule α. On déduit que le reste de cette division est forcément nul. Maintenant, on déduit par le théorème d'isomorphisme que $\mathbb{Z}[t]/(t^3+t+1)$ est isomorphe à un sous-anneau de $\mathbb{R}$, en particulier intègre. Ainsi on conclut que l'idéal (t^3+t+1) est premier.

Exercice 3.
Dans cet exercice, nous étudions les anneaux $\mathbb{Z}[i]/(p)$ pour p un nombre premier. Nous écrirons $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

1. Montrez que $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[t]/(t^2+1)$.
   Indication : Utilisez le quotient en deux temps.

2. Pour $p=5$, montrez que $\mathbb{Z}[i]/(5) \cong \mathbb{F}_5 \times \mathbb{F}_5$.
   Indication : Le théorème des restes chinois peut être utile.

3. Plus généralement montrez que $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p \times \mathbb{F}_p$ si et seulement si $p \equiv 1 \mod 4$.
   Indication: Montrez que l'hypothèse est équivalente à l'existence de deux racines carrés disctintes de -1 dans $\mathbb{F}_p$. Pour une direction, on utilisera que $\mathbb{F}_p^\times$ est un groupe cyclique.[†]

4. Montrez que (p) est premier comme idéal de $\mathbb{Z}[i]$ si et seulement si $p \equiv 2,3 \mod 4$ et $p \neq 2$.

Solution.

1. On sait 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

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

[†]Voici une preuve de ce fait. Si ce groupe n'était pas cyclique, par la classification des groupes abéliens de type fini, il existerait $n < p-1$ tel que $x^n = 1$ pour tout $x \in \mathbb{F}_p^\times$. Mais alors t^n-1 aurait $p-1$ racines dans $\mathbb{F}_p$ ce qui est absurde.

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 comme $(\mathbb{F}_p^\times, \times)$ est cyclique, de générateur disons α, on voit que $\alpha^{\frac{p-1}{4}}$ est d'ordre 4.

Maintenant montrons que $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p \times \mathbb{F}_p$ si et seulement si -1 possède deux racines distinctes modulo p.

Si -1 possède deux racines distinctes dans $\mathbb{F}_p$, disons α_1, α_2, alors $t^2+1 = (t-\alpha_1)(t-\alpha_2)$ et donc comme $\alpha_1 \neq \alpha_2$ on peut utiliser le théorème des restes chinois pour obtenir que

$$\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[t]/(t^2+1) = \mathbb{F}_p[t]/(t-\alpha_1)(t-\alpha_2) \cong \mathbb{F}_p \times \mathbb{F}_p.$$

Réciproquement si

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

notons (α_1, α_2) l'image de t par cet isomorphisme. Comme $t^2 = -1$ dans l'anneau de gauche, on voit que $\alpha_1^2 = \alpha_2^2 = -1$. Il reste à démontrer que $\alpha_1 \neq \alpha_2$. Supposons par l'absurde que ce soit le cas, et que ces éléments soient égaux à un $\lambda \in \mathbb{F}_p$. Mais alors $t-\lambda$ serait dans le noyau de la composition

$$\mathbb{F}[t] \to \mathbb{F}_p[t]/(t^2+1) \cong \mathbb{F}_p \times \mathbb{F}_p$$

et donc inclus dans (t^2+1) comme le deuxième morphisme est un isomorphisme. Mais cela est absurde car un polynôme de degré 2 ne peut diviser un polynôme de degré 1.

4. Si $p \equiv 1 \mod 4$ ou égal à 2, on voit que l'idéal n'est pas premier. En effet dans le premier cas c'est grâce au point précédent: un produit d'anneau non-nuls n'est jamais intègre. Pour $p=2$, on a $\mathbb{Z}[i]/(2) \cong \mathbb{F}_2[t]/(t^2+1) = \mathbb{F}[t]/(t+1)^2$. Cet anneau n'est pas intègre car $t+1$ est non-nul et nul au carré.

   Pour l'autre direction si $p \equiv 2,3 \mod 4$ et $p \neq 2$, on veut montrer que (p) est premier. L'hypothèse sur p est équivalente au fait que -1 n'a pas de racine carrée dans $\mathbb{F}_p$.

   On veut donc montrer que (t^2+1) est premier dans $\mathbb{F}_p[t]$.[‡] Soit $at+b \in \mathbb{F}_p[t]/(t^2+1)$ un élément non-nul. Il suffit de montrer que la multiplication par cet élément est injective, cela donnerait l'intégrité. Un élément du noyau est un $ct+d$ tel que

   $$(at+b)(ct+d) = 0 \in \mathbb{F}_p[t]/(t^2+1).$$

   En relevant cela à $\mathbb{F}_p[t]$ on a

   $$(at+b)(ct+d) = (t^2+1)f(t)$$

   pour un polynôme $f(t) \in \mathbb{F}_p[t]$. En terme de degré, on voit que nécessairement $a, c \neq 0$ et que $\deg(f(t)) = 0$. Mais alors on déduit que $-b/a$ est un zéro de t^2+1 une contradiction car cela impliquerait que -1 aurait une racine carrée dans $\mathbb{F}_p$ une contradiction.

Exercice 4.
Soit un anneau commutatif A où $2 \in A^\times$. Montrez qu'il existe un isomorphisme de A-algèbres (cela signifie que les constantes de $A[t]$ sont envoyées sur les éléments diagonaux de $A \times A$)

$$A[t]/(t^2-1) \cong A \times A.$$

Si $2 \notin A^\times$, alors montrez qu'un tel isomorphisme ne peux exister.

Solution. Comme

$$t-1-(t+1) = -2$$

le premier point est une conséquence du théorème des restes chinois. Pour le deuxième point, on prend $\mathfrak{m}$ un idéal maximal de A avec $2 \in \mathfrak{m}$ par le théorème de Krull. On considère l'idéal généré

[‡]La preuve ci-dessous montre en fait que idéal est maximal. Voir l'exercice sur les algèbres intègres de dimension finie sur un corps.

par $\mathfrak{m}$ vu comme constante et comme éléments diagonaux respectivement dans $A[t]/(t^2-1)$ et $A \times A$. Si on suppose qu'il existe un isomorphisme de A-algèbres entre ces deux anneaux, ces deux idéaux vont coincider par cet isomorphisme et donc induire un isomorphisme

$$(A/\mathfrak{m})[t]/(t^2-1) \to A/\mathfrak{m} \times A/\mathfrak{m}.$$

Mais $A/\mathfrak{m}$ est un corps de caractéristique 2, donc $(t^2-1) = (t-1)^2$. Mais alors le dernier point de l'exercice 1 amène à une contradiction.

Exercice 5.
Soit A un anneau commutatif. On note $\mathrm{nil}(A)$ pour les éléments nilpotents de A. Soit k un corps.

1. Déterminer $\mathrm{nil}(A)$, où $A = k[x,y]\Big/(x^2y^3)$.
2. Écrire $\mathrm{nil}(A)$ comme l'intersection d'idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, $\mathrm{nil}(A) = \cap_{i=1}^m \mathfrak{p}_i$, pour m minimal.
3. Déterminer les premiers minimaux de A.

Solution.

1. Soit $f(x,y) \in k[x,y]/(x^2y^3)$ nilpotent. On écrit $f(x,y) = xyh_1(x,y) + xh_2(x) + yh_2(y) + \lambda$, avec $\lambda \in k$. Comme xy est nilpotent, il suit que $xh_2(x) + yh_2(y) + \lambda$ est nilpotent. Comme l'image dans le quotient par (x) et (y) dans $k[y]$ et $k[x]$ respectivement est encore nilpotente et que ces anneaux sont intègres, il suit que $h_2(x) = h_2(y) = \lambda = 0$. Dès lors on conclut que $\mathrm{nil}(A) = (xy)$.

   On peut aussi utiliser que les éléments nilpotents sont l'intersection de tous les premiers (Théorème mentionné dans les notes du cours). Comme (x) et (y) sont premiers, on a $\mathrm{nil}(A) \subset (x) \cap (y) = (xy)$. Comme l'autre inclusion est également vérifiée, on a égalité.

2. Notons que $(x) \cap (y) = (xy)$. En effet si $f(x,y) \in (x) \cap (y)$ alors $f(x,y) = xh_1(x,y) = yh_2(x,y)$. Comme (x) est un idéal premier, et que $y \notin (x)$ il suit que $h_2(x,y) \in (x)$, et donc que $f(x,y) \in (xy)$. Dès lors $\mathrm{nil}(A) = (x) \cap (y)$. Cette intersection est bien minimale, en effet sinon $\mathrm{nil}(A)$ serait premier. Mais $x, y \notin \mathrm{nil}(A)$ et $xy \in \mathrm{nil}(A)$.

3. Si $\mathfrak{p}$ est un premier qui contient x^2y^3, alors x ou y appartient à $\mathfrak{p}$ comme cet idéal est premier. Ainsi (x) ou (y) est inclus dans $\mathfrak{p}$. Comme ces idéaux sont premiers on conclut que ces premiers sont minimaux. En effet, en utilisant le raisonnement précédent si $\mathfrak{p} \subset (x)$, alors soit $(y) \subset \mathfrak{p} \subset (x)$ ou $(x)\mathfrak{p} \subset (x)$. Dans le deuxième cas, on a $\mathfrak{p} = (x)$. Notez que le premier cas est impossible car $y \notin (x)$. Ainsi (x) est minimal. Un raisonnement symétrique pour y s'applique.