EPFL - Printemps 2025	Prof. Zs. Patakfalvi
Anneaux et Corps	**Exercices**
Solutions 4	

Exercice 1. (a) Soit k un corps. Trouver tous les idéaux de l'anneau quotient $k[t]/(t^2)$. Déterminer lesquels sont premiers et lesquels sont maximaux.

(b) Soit $I \subset M \subset A$ deux idéaux d'un anneau A et soit $\pi : A \to A/I$ l'homomorphisme quotient. Montrer que l'idéal $\pi(M)$ est maximal dans A/I si et seulement si M est maximal dans A.

Solution.

(a) Notons tout d'abord qu'un élément de $x \in k[t]/t^2$ s'écrit uniquement sous la forme $x = \lambda + \mu t$ avec $\lambda, \mu \in k$. Notons aussi qu'un élément est inversible si et seulement si $\lambda \neq 0$. En effet si $\lambda = 0$, on a que x est nilpotent, et si $\lambda \neq 0$, on a $x^{-1} = \lambda^{-1}(1 - \mu\lambda^{-1}t)$. Autrement dit on a $(t) = (k[t]/t^2) \setminus (k[t]/t^2)^\times$. Comme tout idéal propre est inclus dans $(k[t]/t^2) \setminus (k[t]/t^2)^\times = (t)$ (sinon l'idéal contient un inversible et n'est pas propre), on obtient par le théorème de correspondance que les idéaux propres de $k[t]/t^2$ sont en bijection avec les idéaux J de $k[t]$ tel que

$$(t^2) \subset J \subset (t).$$

Mais comme $(t)/(t^2)$ est un k-espace vectoriel de dimension 1, on voit que $J = (t^2)$ ou $J = (t)$.

On conclut que les idéaux sont : l'idéal impropre, l'idéal nul et l'unique idéal maximal (t).

Un autre argument: (t) dans le quotient est un idéal maximal nilpotent. C'est alors l'unique idéal *premier*. Dans l'exercice 6 de la série 3, on montre que c'est l'unique idéal maximal. Mais l'exact même argument fonctionne également pour montrer que c'est l'unique idéal premier.

(b) Let $I \subseteq M \subseteq A$ be two ideal in A. By Proposition 1.4.41 we have that:

$$A/M \cong (A/I)/\pi(M).$$

Now M is a maximal ideal in A if and only if A/M is a field. Now, by the above, A/M is a field if and only if $(A/I)/\pi(M)$ is a field, hence if and only if $\pi(M)$ is a maximal ideal in A/I.

Exercice 2 (Fonctions polynomiales.)**.**
Soit A un anneau commutatif et $\mathcal{F}(A)$ l'anneau des fonctions $\varphi\colon A \to A$ où la somme et le produit sont définis dans l'ensemble d'arrivée (par exemple $(\varphi \cdot \phi)(a) = \varphi(a) \cdot \phi(a)$). On considère l'évaluation comme application $\mathrm{ev}\colon A[t] \to \mathcal{F}(A)$. L'évaluation d'un polynôme f est donc la fonction polynomiale $\mathrm{ev}(f)$ définie par $\mathrm{ev}(f)(a) = \mathrm{ev}_a(f) = f(a)$.

(a) Montrer que l'évaluation est un homomorphisme d'anneaux.

(b) Montrer que si A est fini, alors l'évaluation n'est pas injective.

(c) Montrer que si A est intègre et infini, alors l'évaluation est injective.

Solution.

(a) Let $f(t), g(t) \in A[t]$. We have that

$$\mathrm{ev}(f+g)(a) = (f+g)(a) = f(a) + g(a) = \mathrm{ev}(f)(a) + \mathrm{ev}(g)(a) = (\mathrm{ev}(f) + \mathrm{ev}(g))(a)$$

for all $a \in A$. Therefore $\mathrm{ev}(f+g) = \mathrm{ev}(f) + \mathrm{ev}(g)$.

Similarly,

$$\mathrm{ev}(fg)(a) = (fg)(a) = f(a)g(a) = \mathrm{ev}(f)(a)\,\mathrm{ev}(g)(a) = (\mathrm{ev}(f)\,\mathrm{ev}(g))(a)$$

for all $a \in A$. Therefore $\mathrm{ev}(fg) = \mathrm{ev}(f)\,\mathrm{ev}(g)$.

Lastly, we have that $\mathrm{ev}(1)(a) = 1$ for all $a \in A$ and thus $\mathrm{ev}(1) = 1$, where the constant polynomial function 1 is the unity of $\mathcal{F}(A)$.

(b) Consider the polynomial $f(t) = \prod_{a\in A}(t-a)$. Then $f \neq 0 \in A[t]$, but $f(a) = 0$ for all $a \in A$.

(c) Supposons que A est intègre et infini. Soit f dans le noyau. Alors f s'annule en tous les $a \in A$. Prenons une suite infinie d'éléments distincts $a_1, \ldots, a_n, \ldots$. Notons que $(t-a_1) \mid f$. Donc

$$f = g(t-a_1).$$

Donc $f(a_2) = g(a_2)(a_2 - a_1)$. Comme $a_2 \neq a_1$ et A est intègre, on a $g(a_2) = 0$. Alors $(t-a_2) \mid g$. Par récurence, on voit que $(t-a_n) \mid f$ pour tout n. Ainsi on voit que forcément $f = 0$, sans quoi le degré de ce polynôme ne serait pas borné.

Exercice 3.
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 2.5.17). 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.

Exercice 4.
Montrer que $\mathbb{F}_p[x]/(x^p - 1)$ n'est pas isomorphe à un produit de deux anneaux non-nuls.

Solution.

Notons que $(t^p - 1) = (t^p + (-1)^p) = (t-1)^p$.* Dès lors

$$A := \mathbb{F}_p[t]/(t-1)^p = \mathbb{F}_p[t]/(t^p - 1)$$

Première solution.

Notez que l'évaluation $\mathbb{F}_p[t] \xrightarrow{t\mapsto 1} \mathbb{F}_p$ passe au quotient

$$A \xrightarrow{t\mapsto 1} \mathbb{F}_p$$

car $(t-1)^p$ est envoyé su zéro. Prenons maintenant un idempotent $e \in A$, c'est à dire que $e^2 = e$. Notez que si $f(t)$ est un lift de e dans $\mathbb{F}_p[t]$, on peut écrire

$$f(t) = f(1) + (t-1)g(t)$$

par division euclidienne.

Notez que que comme $(t-1)^p = 0$ et que $(-)^p$ est un morphisme en caractéristique p on peut dès lors écrire

$$e = \lambda + n$$

pour $\lambda \in \mathbb{F}_p$ et $n \in A$ tel que $n^p = 0$. Comme $e^p = e$ on obtient

$$\lambda + n = \lambda^p + n^p = \lambda$$

car $n^p = 0$ et $\lambda^p\lambda$ comme $\lambda \in \mathbb{F}_p$. On en déduit que $n = 0$. Comme dès lors on sait aussi que $\lambda^2 = \lambda$, on voit que $\lambda = 0, 1$ ce qui conclut que les seuls idempotents sont $0, 1$ et donc que A n'est pas un produit d'anneaux non-nuls.

Deuxième solution.

Rappelons que selon l'exercice 6 de la série 3, si $A \setminus A^\times$ est un idéal, alors c'est l'unique idéal maximal de A.

Maintenant, notons qu'un produit d'anneaux $A \times B$ non-nuls contient toujours au-moins deux idéaux maximaux : si $\mathfrak{m}_A$ et $\mathfrak{m}_B$ sont des idéaux maximaux de A et B respectivement, alors $\mathfrak{m}_A \times B$ et $A \times \mathfrak{m}_B$ sont maximaux.

Maintenant, dans l'anneau

$$A = \mathbb{F}_p[t]/(t-1)^p = \mathbb{F}_p[t]/(t^p - 1),$$

notons que $t - 1$ est nilpotent. Si $f(t) \in \mathbb{F}_p[t]$, on peut écrire

$$f(t) = f(1) + (t-1)g(t)$$

par division euclidienne. Ainsi l'image dans le quotient $\overline{f(t)}$ peut s'écrire $\overline{f(t)} = f(1) - n$ avec $n \in A$ nilpotent. Dès lors, on voit que† $\overline{f(t)}$ est inversible si et seulement si $f(1) \neq 0$ ou autrement dit $\overline{f(t)} \notin (\bar{t} - 1) = \ker(ev_1)$. Ainsi on a $A \setminus A^\times = (\bar{t} - 1)$ qui est un idéal, et donc l'unique idéal maximal. Dès lors, il suit que A ne peut être un produit de deux anneaux non-nuls.

Exercice 5.
L'anneau $\mathbb{Z}[\sqrt{5}]$.

1. Montrer que la norme $N\colon \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}$ définie par $N(a + b\sqrt{5}) = a^2 - 5b^2$ est une fonction multiplicative (donc que $N(xy) = N(x)N(y)$ – noter que si l'on définit $\overline{a + b\sqrt{5}} = a - b\sqrt{5}$, alors $N(x) = x\overline{x}$) et que $a + b\sqrt{5}$ est inversible si et seulement si $N(a + b\sqrt{5}) = \pm 1$.

*Cet argument marche aussi en caractéristique 2 car dès lors $1 = -1$.

†si $\lambda \in A^\times$ et $n \in A$ nilpotent, alors $\lambda - n$ est inversible. En effet,

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

2. Montrer que $9+4\sqrt{5}$ est inversible et en déduire que $(\mathbb{Z}[\sqrt{5}])^\times$ est infini.

3. Montrer qu'il n'existe aucun élément de norme 2 ou -2, si bien que tout élément de norme 4 est irréductible.

4. Trouver deux décompositions de 4 en produit d'irréductibles dans $\mathbb{Z}[\sqrt{5}]$.

5. L'idéal $(3+\sqrt{5})$ est-il premier?

Solution.

1. We define $\overline{a+b\sqrt{5}} = a-b\sqrt{5}$ and note that for all $z \in \mathbb{Z}[\sqrt{5}]$, the norm $N(z) = z\overline{z}$. The fact that N is a multiplicative function then follows from the fact that $\forall y, z \in \mathbb{Z}[\sqrt{5}]$, it holds that $\overline{yz} = \overline{y}\,\overline{z}$. With this, we get that $N(yz) = yz\overline{yz} = yz\overline{y}\,\overline{z} = y\overline{y}z\overline{z} = N(y)N(z)$.

   Furthermore, if $z \in \mathbb{Z}[\sqrt{5}]$ is invertible, then $N(z) = \pm 1$ is necessary. If we denote its inverse by z^{-1}, then $N(z)N(z^{-1}) = N(1) = 1$, and therefore, $N(z) = \pm 1$. On the other hand, if $N(z) = \pm 1$ for some $z \in \mathbb{Z}[\sqrt{5}]$, then $\pm 1 = N(z) = z\overline{z}$ and hence $\pm\overline{z}$ is the inverse of z.

2. We note that $N(9+4\sqrt{5}) = 9^2 - 5\cdot 4^2 = 1$, and so by the first point, $9+4\sqrt{5}$ is invertible. Furthermore, by the multiplicative property of the norm, the norm of $(9+4\sqrt{5})^n$ is 1 as well, for $n \in \mathbb{N}$. This means that we have created infinitely many invertible elements, and $(\mathbb{Z}[\sqrt{5}])^\times$ is infinite.

3. We first show that no elements of norm 2 exist. For this, we note that $N(a+\sqrt{5}b) = a^2 - 5b^2$, which is equal to a^2 modulo 5, a square. But all squares in $\mathbb{Z}/5\mathbb{Z}$ are either 0,1 or 4, as one checks by taking the square of all elements in $\mathbb{Z}/5\mathbb{Z}$.

   Now let $z \in \mathbb{Z}[\sqrt{5}]$ be of norm 4, and we assume that $z = v \cdot w$ for $v, w \in \mathbb{Z}[\sqrt{5}]$. Then $4 = N(z) = N(v)N(w)$. But as there are no elements of norm 2, we have that either $N(v) = \pm 1, N(w) = \pm 4$ or $N(v) = \pm 4, N(w) = \pm 1$. In either cases one of the two elements is of norm ± 1, which means that that element is invertible. Hence z is irreducible.

4. We have

   - $4 = 2\cdot 2$ and $N(2) = 4$, hence by the previous part, 2 is irreducible
   - $4 = (1+\sqrt{5})(-1+\sqrt{5})$ and $N(1+\sqrt{5}) = -4, N(-1+\sqrt{5}) = -4$, hence both $1+\sqrt{5}, -1+\sqrt{5}$ are irreducible.
   - $4 = (3+\sqrt{5})(3-\sqrt{5})$ and $N(3+\sqrt{5}) = 4, N(3-\sqrt{5}) = 4$, hence both $3+\sqrt{5}, 3-\sqrt{5}$ are irreducible.

5. As we see from the previous point, $2\cdot 2 = 4 = (3+\sqrt{5})(3-\sqrt{5})$, from which it follows that $2\cdot 2 \in (3+\sqrt{5})$. But as $2 \notin (3+\sqrt{5})$, the ideal $(3+\sqrt{5})$ is not prime.

   We remark (all these notions will be defined later in the course) that irreducible does not imply prime in a ring that is not factorial or principal.

Exercice 6.
Soit $d > 1$. On note $A = \mathbb{Z}[i\sqrt{d}]$. On note $N(a+bi\sqrt{d}) = a^2 + db^2$.

1. Lister les éléments $x \in A$ tel que $N(x) \leq d+1$.

2. Montrer que $i\sqrt{d}$, $1+i\sqrt{d}$ et $1-i\sqrt{d}$ sont irréductibles.

3. Si $d+1$ n'est pas premier *dans* $\mathbb{Z}$, alors A n'est pas factoriel.

4. Si $q = d+1$ est premier *dans* $\mathbb{Z}$ alors celui-ci admet une factorisation unique en irréductibles dans A.

Solution.

1. Soit $x = a + bi\sqrt{d} \in A$ avec $a^2 + b^2 d \leq d + 1$. Donc

$$a^2 + (b^2 - 1)d \leq 1.$$

On voit dès lors que $|b| \leq 1$. On distingue deux cas. Tout d'abord traitons le cas où $b = \pm 1$. Alors on a nécessairement $a = 0$ ou $a = \pm 1$, c'est à dire

$$x = \pm i\sqrt{d} \quad x = \pm(1 - i\sqrt{d}) \quad x = \pm(1 + i\sqrt{d}).$$

Traitons maintenant le cas où $b = 0$. On alors $x = a \in \mathbb{Z}$ avec la condition que $|a| \leq \sqrt{1 + d}$.

2. On montre d'abord que $i\sqrt{d}$ est irréductible. On a $N(i\sqrt{d}) = d$. Ainsi si $x \mid i\sqrt{d}$ avec x ni inversible ni associé, il faut que $1 < N(x) < d$. Selon la liste établie au point 1, on a alors $x = a \in \mathbb{Z}$ avec $|a| < \sqrt{d}$. Mais comme on a supposé que $x \mid i\sqrt{d}$, il existe $e, f \in \mathbb{Z}$ tel que

$$a(e + fi\sqrt{d}) = i\sqrt{d}.$$

Donc $e = 0$ et $fa = 1$ ce qui contredit $N(a) > 1$.

On montre maintenant que $1 + i\sqrt{d}$ est irréductible. Comme la conjugaison complexe est un automorphisme d'anneau qui envoie $1 + i\sqrt{d}$ sur $1 - i\sqrt{d}$ cela montrera que $1 - i\sqrt{d}$ est également irréductible. Comme $N(1 + i\sqrt{d}) = 1 + d$, si $x \mid 1 + i\sqrt{d}$ avec x ni irréductible ni associé à $1 + i\sqrt{d}$, alors $1 < N(x) < 1 + d$. Comme il faut aussi que $N(x) \mid 1 + d$, on voit que $N(x) < d$. Ainsi un argument similaire à celui au-dessus conclut.

3. Supposons que $1 + d$ n'est pas premier dans $\mathbb{Z}$. Alors on a

$$1 + d = (1 + i\sqrt{d})(1 - i\sqrt{d}) = p_1 \cdots p_r$$

pour $p_1, \ldots, p_r$ des premiers avec $p_i \leq d$ comme on a supposé $d + 1$ pas premier. Comme $1 + i\sqrt{d}$ est irréductible, si $1 + d$ admet une factorisation *unique* en produit d'irréductibles (en supposant par l'absurde que A est factoriel) cela impliquerait que $1 + i\sqrt{d} \mid p_j$ pour un indice j. Mais dès lors il existerait $e, f \in \mathbb{Z}$ avec

$$(1 + i\sqrt{d})(e + fi\sqrt{d}) = p_j$$

Donc $e + f = 0$ et $p_j = e - df = (1 + d)e$. Comme $p_j \leq d$, c'est une contradiction. Ainsi on conclut que $1 + d$ n'admet pas de factorisation unique en produit d'irréductibles. En particulier, on conclut que dans ce cas A n'est pas factoriel.

4. Supposons maintenant $q := 1 + d$ premier dans $\mathbb{Z}$. On a

$$1 + d = (1 + i\sqrt{d})(1 - i\sqrt{d}),$$

qui est une décomposition en irréductibles. On veut montrer que si $x \mid 1 + d$ et est ni inversible ni associé à $1 + d$, alors x est associé à $1 + i\sqrt{d}$ ou $1 - i\sqrt{d}$. Comme $N(1 + d) = (1 + d)^2 = q^2$, un tel diviseur x satisfait forcément $N(x) = q = 1 + d$. Selon la liste au-dessus on a dès lors

$$x = \pm(1 - i\sqrt{d}) \quad x = \pm(1 + i\sqrt{d}).$$

ou $x \in \mathbb{Z}$ avec $x^2 = q$, mais cela n'est pas possible comme q est premier.