TD 9 : corrigé

1. Sous-anneaux

Tout anneau intègre peut-être vu comme un sous-anneau de son corps des fractions, qui est noethérien et factoriel de manière tautologique. Tout exemple d'anneau intègre mais pas noethérien (resp. factoriel) répond donc à la question. Des exemples sont d'ailleurs donnés dans le TD dans les exercices 3 et 4.

2. Décomposition dans les anneaux noethériens

Attention, l'hypothèse d'intégrité a été oubliée dans l'énoncé de la feuille de TD. Elle est pourtant primordiale : dans $\mathbb{Z}/6\mathbb{Z}$ (évidemment noethérien, car fini), les seuls inversibles sont $\overline{1}$ et $\overline{5}$ et les relations $\overline{2} = \overline{4} \times \overline{2}$, $\overline{3} = \overline{3} \times \overline{3}$ et $\overline{4} = \overline{2} \times \overline{2}$ prouvent qu'il n'y a pas d'élément irréductible. De manière générale, il vaut mieux ne parler d'éléments irréductibles que dans un anneau intègre.

Convenons qu'un élément $x \in \mathrm{A}$ est dit *finiment décomposable* s'il s'écrit comme un produit fini d'éléments irréductibles. Supposons *ad absurdum* qu'il existe un élément $x \in \mathrm{A}$ non finiment décomposable. Construisons par récurrence une suite de couples d'éléments de (a_n, b_n) de A vérifiant :

- pour tout $n \geqslant 0$, $x = a_n b_n$;
- a_n n'est finiment décomposable pour aucun $n \geqslant 0$;
- pour tout $n \geqslant 0$, a_{n+1} divise a_n strictement (c'est-à-dire qu'il ne lui est pas associé).

La construction est immédiate : d'abord $a_0 = x$ et $b_0 = 1$. Ensuite, si on suppose la construction réalisée à l'étape n, on a que a_n n'est pas irréductible (il serait alors finiment décomposable) : on peut donc l'écrire $a_n = s_n t_n$ avec s_n et t_n non inversibles. Ces deux éléments divisent donc strictement a_n. Puisque a_n n'est pas finiment décomposable, au moins l'un des deux, disons s_n, ne l'est pas non plus. On pose alors $a_{n+1} = s_n$ et $b_{n+1} = b_n t_n$, qui vérifient bien les hypothèses.

On a déjà vu que dans un anneau intègre, si a' divise a sans lui être associé, l'inclusion $(a) \subset (a')$ est stricte. [1] Notre construction fournit alors une suite infinie strictement croissante $(a_n) \subset (a_{n+1})$, ce qui contredit directement l'hypothèse de noethérianité de A.

6. Valuation dans A[X]

1. Par définition, si v est la valuation de P, ce dernier s'écrit $\mathrm{P} = a_v \mathrm{X}^v + \widetilde{\mathrm{P}}$ où $a_v \neq 0$ et $\widetilde{\mathrm{P}}$ est composé des termes de degré $\geqslant v+1$; on peut donc réécrire $\mathrm{P} = a_v \mathrm{X}^v + \mathrm{X}^{v+1}\mathrm{P}'$ pour un

1. Rappelons-en la preuve : par hypothèse, $a = sa'$. Si l'inclusion $(a) \subset (a')$ était une égalité, on aurait également un élément $t \in \mathrm{A}$ tel que $a' = ta$. En les combinant, on obtient $a = sta$, d'où $(st-1)a = 0$ et, par intégrité, $st = 1$, ce qui donne s inversible et a et a' associés.

certain polynôme $P' \in A[X]$. Ainsi, P est divisible par X^v et il ne peut pas être divisible par X^{v+1}, car alors $a_v X^v$ le serait. La valuation $v = \operatorname{val} P$ est donc bien le plus grand k tel que X^k divise P.
2. Un polynôme de valuation v s'écrit sous la forme $P = a_v X^v + X^{v+1} P'$, avec $a_v \in A \setminus \{0\}$ et $P' \in A[X]$. Écrivons Q sous la même forme : $Q = b_w X^w + X^{w+1} Q'$. On a alors [2]

$$PQ = a_v b_w X^{v+w} + X^{v+w+1} R,$$

pour $R = a_v Q' + b_w P' + XP'Q' \in A[X]$. Puisque, par intégrité, $a_v b_w \neq 0$, on a bien

$$\operatorname{val}(PQ) = v + w = \operatorname{val}(P) + \operatorname{val}(Q).$$

7. Critère d'Eisenstein

1.

(a) Écrivons une décomposition de P dans K[X] : $P = \widetilde{P}_1 \cdot \widetilde{P}_2$. On peut trouver des éléments Δ_i de A tels que les produits $\Delta_i P_i$ soient des polynômes de A[X]. On a donc une décomposition dans A[X] : $\Delta_1 \Delta_2 P = (\Delta_1 \widetilde{P}_1)(\Delta_2 \widetilde{P}_2)$. Le lemme de Gauß implique donc que $\operatorname{cont}(\Delta_1 \Delta_2 P) = \Delta_1 \Delta_2 \operatorname{cont}(P)$ est associé au produit $\operatorname{cont}(\Delta_1 P_1) \operatorname{cont}(\Delta_2 P_2)$. On a donc

$$P = \operatorname{cont}(P) \frac{\Delta_1 \Delta_2 P}{\operatorname{cont}(\Delta_1 \Delta_2 P)} = \operatorname{cont}(P) \frac{\Delta_1 \widetilde{P}_1}{\operatorname{cont}(\Delta_1 \widetilde{P}_1)} \frac{\Delta_2 \widetilde{P}_2}{\operatorname{cont}(\Delta_2 \widetilde{P}_2)},$$

ce qui est bien une décomposition dans A[X].

(b) Une fois réduit modulo I, le polynôme $\overline{P}$ est, d'après le premier point du critère d'Eisenstein, un simple monôme de degré $\deg P$. Autrement dit, on a $\deg \overline{P} = \operatorname{val} \overline{P} = \deg P$. D'après la formule d'additivité du degré et celle, démontrée plus haut, de la valuation, les réductions modulo I des polynômes P_1 et P_2 vérifient

$$\operatorname{val} \overline{P} = \operatorname{val} \overline{P}_1 + \operatorname{val} \overline{P}_2 \leqslant \deg \overline{P}_1 + \deg \overline{P}_2 \leqslant \deg P_1 + \deg P_2 = \deg P = \operatorname{val} \overline{P}.$$

Toutes les inégalités sont donc des égalités et on a $\deg \overline{P}_1 = \operatorname{val} \overline{P}_1 = \deg P_1$, ce qui est une reformulation du premier point du critère d'Eisenstein (et bien entendu, la même chose est vraie pour P_2). Puisque P_1 et P_2 vérifient le premier point du critère d'Eisenstein, leurs coefficients constants sont dans I. Le coefficient de leur produit, qui est évidemment le produit des coefficients constants est alors dans I^2, ce qui contredit le second point du critère d'Eisenstein. On est donc arrivé à une contradiction, ce qui démontre *ad absurdum* que P était bien irréductible dans K[X].

2. Le polynôme $2X + 6$ est réductible dans $\mathbb{Z}[X]$ (il s'écrit $2 \cdot (X + 3)$) mais il satisfait le critère d'Eisenstein pour $I = 3\mathbb{Z}$.
3. Que P soit irréductible si et seulement si $P(X + 1)$ l'est est à peu près évident. On peut par exemple argüer que $P \mapsto P(X + 1)$ est un automorphisme d'anneaux (d'inverse $P \mapsto P(X - 1)$) et qu'il doit donc envoyer irréductibles sur irréductibles.

Si $P = X^{p-1} + X^{p-2} + \cdots + X + 1 = \dfrac{X^p - 1}{X - 1}$, le polynôme $P(X + 1)$ s'écrit donc

$$P(X + 1) = \frac{(X + 1)^p - 1}{X} = X^{p-1} + \binom{p}{1} X^{p-2} + \binom{p}{2} X^{p-3} + \cdots + \binom{p}{p-1}.$$

2. L'envie est presque irrésistible de noter ces expressions sous la forme $P = a_v X^v + O(X^{v+1})$, etc.

Il vérifie bien le critère d'Eisenstein pour l'idéal $I = p\mathbb{Z}$, en utilisant les congruences classiques

$$\forall 1 < k < p, \binom{p}{k} \equiv 0 \mod p$$

et est donc irréductible dans $\mathbb{Q}[X]$. Puisqu'il est primitif, il est irréductible dans $\mathbb{Z}[X]$.

8. Idéaux de $\mathbb{Z}[X]$

1. Soit $I \subset \mathbb{Z}[X]$ un idéal premier *strict*, c'est-à-dire différent de (0) et $\mathbb{Z}[X]$.

(a) On peut facilement vérifier à la main que $I \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. Remarquons qu'en fait c'est également l'image réciproque de I par le morphisme d'inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[X]$ et que c'est donc un idéal premier.[3] S'il était égal à tout $\mathbb{Z}$, I contiendrait 1 et serait donc $\mathbb{Z}[X]$ tout entier, ce qui est explicitement exclu par l'énoncé.

(b) i. On a bien évidemment $I \subset \widetilde{I} \cap \mathbb{Z}[X]$. Reste à démontrer l'inclusion réciproque. Soit donc $P \in \widetilde{I} \cap \mathbb{Z}[X]$. Par définition, P s'écrit comme une combinaison finie $P = \sum Q_i P_i$, avec $Q_i \in \mathbb{Q}[X]$ et $P_i \in I$. On peut alors trouver un entier $n \in \mathbb{Z}$ tel que pour tout i, $nQ_i \in \mathbb{Z}[X]$ (le pgcd des dénominateurs de tous les coefficients des (Q_i) convient, par exemple). On a alors $nP = \sum (nQ_i)P_i \in I$. Mais par primalité de I, cela implique $n \in I$ (exclu car $I \cap \mathbb{Z} = (0)$) ou $P \in I$, ce que l'on voulait démontrer.

ii. L'anneau $\mathbb{Q}[X]$ étant principal, l'idéal $\widetilde{I}$ est engendré (en tant qu'idéal de $\mathbb{Q}[X]$) par un polynôme $\widetilde{P}$. Si n est le pgcd des dénominateurs des coefficients de $\widetilde{P}$, $n\widetilde{P}$ est un polynôme entier et, en posant $r = \dfrac{n}{\mathrm{cont}(n\widetilde{P})} \in \mathbb{Q}$, $P = r\widetilde{P}$ est un polynôme entier primitif appartenant à $\widetilde{I}$.

On a alors évidemment $(P)_{\mathbb{Z}[X]} = (r\widetilde{P})_{\mathbb{Z}[X]} \subset (\widetilde{P})_{\mathbb{Q}[X]} \cap \mathbb{Z}[X]$, qui est égal à I d'après la question précédente. Pour démontrer l'inclusion réciproque, prenons un élément de $(\widetilde{P})_{\mathbb{Q}[X]} \cap \mathbb{Z}[X]$: il s'écrit $\widetilde{P}\widetilde{Q} = P\widetilde{Q}/r \in \mathbb{Z}[X]$ pour un certain $\widetilde{Q} \in \mathbb{Q}[X]$. Or, une des conséquences du lemme de Gauß est que si P est primitif et $Q \in \mathbb{Q}[X]$, on a l'implication $PQ \in \mathbb{Z}[X] \Rightarrow Q \in \mathbb{Z}[X]$. En effet, si $\Delta \in A$ est tel que $\Delta Q \in A[X]$, on a d'après le lemme de Gauß $\mathrm{cont}(\Delta PQ) = \Delta\,\mathrm{cont}(PQ) = \mathrm{cont}(P)\mathrm{cont}(\Delta Q) = \mathrm{cont}(\Delta Q)$ par primitivité de P. On peut donc écrire

$$Q = \frac{\Delta Q}{\Delta} = \mathrm{cont}(PQ)\frac{\Delta Q}{\mathrm{cont}(\Delta Q)} \in A[X].$$

On a donc $\widetilde{Q}/r \in \mathbb{Z}[X]$ et on a écrit notre élément de $(\widetilde{P})_{\mathbb{Q}[X]} \cap \mathbb{Z}[X]$ sous la forme PQ, $Q \in \mathbb{Z}[X]$ ce qui prouve qu'il appartient à $(P)_{\mathbb{Z}[X]}$: $I = (P)_{\mathbb{Z}[X]}$.

Il reste à voir que P est irréductible. Si P se décompose sous la forme RS, on a $RS \in I$ d'où, par primalité, $R \in I$ ou $S \in I$. Le polynôme R (resp. S) est alors à la fois un multiple et un diviseur de P, ce qui implique (en considérant le degré) que S (resp. R) est un polynôme constant. P étant primitif, cette constante ne peut être que ± 1, c'est-à-dire un inversible de $\mathbb{Z}[X]$. La décomposition de départ était triviale : P est irréductible.

3. On a déjà vu que l'image réciproque d'un idéal était toujours un idéal. Il est facile de voir que cette construction préserve la primalité : $xy \in f^{-1}[I] \Rightarrow f(xy) = f(x)f(y) \in I \Rightarrow f(x)$ ou $f(y) \in I \Rightarrow x$ ou $y \in f^{-1}[I]$.

(c) i. La réduction φ modulo p est un morphisme surjectif, que l'on peut donc voir comme le quotient par un idéal (ici, l'idéal est simplement (p)). Dans ce cadre, l'exercice 8 du TD 7 assure que les idéaux de $\mathbb{F}_p[X]$ sont exactement les images des idéaux contenant (p), et que cette correspondance préserve la primalité (car le quotient reste le même). Puisque I contient p et donc (p), tout cela s'applique et $\varphi[I]$ est un idéal premier de $\mathbb{F}_p[X]$.

ii. Puisque $\mathbb{F}_p[X]$ est principal, on a soit $\varphi[I] = (0)$, soit $\varphi[I] = (\overline{P})$, avec $\overline{P} \in \mathbb{F}_p[X]$ irréductible. Dans le premier cas, on a évidemment $I = \ker\varphi = (p)$; dans le second, si P est un relevé de $\overline{P}$ dans $\mathbb{Z}[X]$, les idéaux (P, p) et $I \lhd \mathbb{Z}[X]$ contiennent (p) et s'envoient par φ sur $\varphi[I]$, donc, d'après la correspondance bijective déja citée, on a $I = (P, p)$, ce qui, puisque P a bien une réduction modulo p irréductible, démontre bien le résultat recherché.

2. Le quotient $\mathbb{Z}[X]/(p) \simeq \mathbb{F}_p[X]$ n'est pas un corps : (p) n'est donc pas un idéal maximal. En revanche, (p, P) est l'image réciproque de $(\overline{P}) \lhd \mathbb{F}_p[X]$, qui est un idéal maximal puisque $\overline{P}$ est irréductible et que $\mathbb{F}_p[X]$ est principal. La correspondance bijective utilisée à la question précédente respectant la maximalité, $(p, P) \lhd \mathbb{Z}[X]$ est un idéal maximal.

Reste à montrer que si P est irréductible dans $\mathbb{Z}[X]$, l'idéal (P) n'est pas maximal. Supposons en effet par l'absurde qu'il le soit et prenons un nombre premier q ne divisant pas le coefficient dominant de P. Puisque q n'appartient pas à (P), on a par maximalité $(q, P) = \mathbb{Z}[X]$ et on peut trouver une relation de Bézout :

$$\exists U, V \in \mathbb{Z}[X] : qU + PV = 1.$$

Mais cela implique qu'après réduction modulo q, P devient inversible dans $\mathbb{F}_p[X]$: $\overline{PV} = 1$. Or, puisque q ne divise pas le coefficient dominant de P, $\overline{P}$ n'est pas un polynôme constant, ce qui constitue la contradiction.

En résumé, *les idéaux premiers de* $\mathbb{Z}[X]$ *sont l'idéal nul, les idéaux principaux* (p) *pour un nombre premier* $p \in \mathbb{Z}$ *et* (P) *pour un polynôme irréductible* $P \in \mathbb{Z}[X]$ *et les idéaux maximaux* (p, P) *où* p *est un nombre premier et* P *un polynôme dont la réduction dans* $\mathbb{F}_p[X]$ *est irréductible.*