Institut Mathématique, Université de Rennes 1
Maîtrise de Mathématiques

ALGEBRE COMMUTATIVE

Corrigé de contrôle du 23 novembre 1996

1. a. Faux. L'idéal $2\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$ et $(\mathbb{Z}\times\mathbb{Z})/(2\mathbb{Z}\times 2\mathbb{Z})$ est isomorphe à l'anneau $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ qui n'est pas intègre. D'où $2\mathbb{Z}\times 2\mathbb{Z}$ n'est pas premier.

b. Faux. 10 est inversible dans l'anneau $\mathbb{Z}/3\mathbb{Z}$. Evidemment, l'anneau fini $\mathbb{Z}/3\mathbb{Z}$ ne contient pas de sous-anneau isomorphe à l'anneau infini des décimaux.

c. Vrai. Lorsque $(a,b)^n=0$ dans $A\times B$, on a $a^n=0$ dans A et $b^n=0$ dans B. Comme A et B sont réduits, $a=0$ et $b=0$. D'où $(a,b)=0$.

d. Faux. $3X^2-15X+6=3\cdot(X^2-5X+2)$ et 3 n'est ni inversible dans $\mathbb{Z}[X]$ ni associé à $3X^2-15X+6$ dans $\mathbb{Z}[X]$, car $\mathbb{Z}[X]^\star=\{\pm 1\}$.

2. a. A est le produit fibré de deux copies de l'anneau $\mathbb{Z}$ sur $\mathbb{Z}/2\mathbb{Z}$ (voir Exercice 50.a).

b. Les deux projections de $\mathbb{Z}\times\mathbb{Z}$ dans $\mathbb{Z}$ sont des morphismes d'anneaux. Par conséquent, leurs restrictions à A, pr_1 et pr_2, sont des morphismes d'anneaux (voir aussi Exercice 50.b).

c. Le quotient $A/\ker(pr_1)$ est isomorphe à un sous-anneau de $\mathbb{Z}$. Or $\mathbb{Z}$ est intègre, donc $A/\ker(pr_1)$ est intègre, c-à-d, $\ker(pr_1)$ est premier. De même, $\ker(pr_2)$ est premier.

d. Soit $I=\ker(pr_1)$ et $J=\ker(pr_1)+A(p,p)$. Alors, $I\subseteq J$. D'après Exercice 79, on a $A/J\cong(A/I)/(J/I)$. Or $pr_1\colon A\to\mathbb{Z}$ est un quotient de A par $I=\ker(pr_1)$, et $J/I=pr_1(J)=p\mathbb{Z}$. D'où $(A/I)/(J/I)\cong\mathbb{Z}/p\mathbb{Z}$. Par conséquent, A/J est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, et est donc un corps. L'idéal $\ker(pr_1)+A(p,p)$ est alors maximal. De même, $\ker(pr_2)+A(p,p)$ est un idéal maximal.

e. Supposons que $\ker(pr_1)+A(p,p)=\ker(pr_2)+A(p,p)$. Prendre l'image par pr_1 donne

$$\begin{aligned}p\mathbb{Z}&=pr_1(\ker(pr_1)+A(p,p))=pr_1(\ker(pr_2)+A(p,p))=\\&=2\mathbb{Z}+p\mathbb{Z}=\operatorname{pgcd}(2,p)\mathbb{Z},\end{aligned}$$

car $\ker(pr_2)=2\mathbb{Z}\times\{0\}\subseteq A$. D'où $p=2$.
Réciproquement, soit $p=2$. Montrons que

$$\ker(pr_1)+A(2,2)=\ker(pr_2)+A(2,2).$$

Il suffit de montrer que $\ker(pr_1) \subseteq \ker(pr_2)+A(2,2)$ et que $\ker(pr_1)+A(2,2) \supseteq \ker(pr_2)$. Pour montrer la première inclusion, soit $a \in \ker(pr_1)$. Alors, $a = (0,n)$ avec $n \in 2\mathbb{Z}$. Il existe $k \in \mathbb{Z}$ tel que $n = 2k$. On a $a = (0,n) = (0,2k) = (-2k,0) + (k,k)(2,2) \in \ker(pr_2) + A(2,2)$. On montre l'autre inclusion pareillement.

f. On a $\ker(pr_1)\cdot\ker(pr_2) = (0)$. Par conséquent, $\ker(pr_1)\cdot\ker(pr_2) \subseteq P$. D'après Proposition 1.7.16, $\ker(pr_1) \subseteq P$ ou bien $\ker(pr_2) \subseteq P$.

g. D'après le c, $\ker(pr_1)$ et $\ker(pr_2)$ sont des idéaux premiers. Montrons qu'ils sont des premiers minimaux. Soit $P \subseteq \ker(pr_1)$ un idéal premier de A. D'après le f, P contient $\ker(pr_1)$ ou $\ker(pr_2)$. Dans ce dernier cas on aurait $\ker(pr_2) \subseteq P \subseteq \ker(pr_1)$ ce qui est absurde. Donc, $\ker(pr_1) \subseteq P$, i.e., $P = \ker(pr_1)$. Cela montre que $\ker(pr_1)$ est un idéal premier minimal. De même, $\ker(pr_2)$ est un idéal premier minimal.

Ensuite, il faut encore montrer que tout idéal premier minimal P de A est égal à $\ker(pr_1)$ ou $\ker(pr_2)$. Or, P est un idéal premier donc P contient $\ker(pr_1)$ ou $\ker(pr_2)$, d'après le f. D'après le c, $\ker(pr_1)$ et $\ker(pr_2)$ sont des idéaux premiers, P étant un idéal premier minimal, P est alors égal à $\ker(pr_1)$ ou $\ker(pr_2)$.

h. D'après le f, P contient $\ker(pr_1)$ ou $\ker(pr_2)$. On montre que $P = \ker(pr_1) + A(p,p)$ pour un unique nombre premier $p \in \mathbb{N}$ lorsque P contient $\ker(pr_1)$. On montre pareillement que $P = \ker(pr_2)+A(p,p)$ lorsque P contient $\ker(pr_2)$.

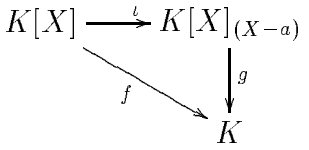
Supposons donc que P contient $\ker(pr_1)$. On a que $P' = pr_1(P)$ est un idéal maximal de $\mathbb{Z}$. Effectivement, $pr_1^{-1}(P') = P + \ker(pr_1) = P$ car $\ker(pr_1) \subseteq P$ (voir Exercice 60.d pour la première égalité). D'où $A/P \cong \mathbb{Z}/P'$. Comme P est maximal, A/P est un corps, et donc $\mathbb{Z}/P'$ est un corps, c-à-d, P' est maximal. Par conséquent il existe un nombre premier $p \in \mathbb{N}$ tel que $P' = p\mathbb{Z}$.

Montrons que $\ker(pr_1) + A(p,p) = pr_1^{-1}(p\mathbb{Z})$. Evidemment, on a que $pr_1(A(p,p)) = p\mathbb{Z}$. D'après Exercice 60.d, on a alors $pr_1^{-1}(p\mathbb{Z}) = \ker(pr_1) + A(p,p)$.

Par conséquent, $P = pr_1^{-1}(P') = pr_1^{-1}(p\mathbb{Z}) = \ker(pr_1) + A(p,p)$. De plus, le nombre premier $p \in \mathbb{N}$ est uniquement déterminé par l'idéal maximal P car p est égal à la caractéristique du quotient A/P.

3. a. $K[X]_{(X-a)}$ est la localisation de $K[X]$ par la partie multiplicative $S = K[X]\backslash(X-a)$. Soit $Q \in S$. Comme Q n'est pas un multiple de $X-a$, $f(Q) = Q(a) \neq 0$. Or, K est un corps, d'où $f(Q)$ est inversible dans K. D'après la propriété universelle de la localisation,

il existe un morphisme g de $K[X]_{(X-a)}$ dans K tel que le diagramme



commute, où ι est le morphisme de localisation. On a alors $g(\frac{P}{1}) = f(P)$ quel que soit $P \in K[X]$.

b. Soit $\frac{P}{Q} \in K[X]_{(X-a)}$, i.e., $P \in K[X]$ et $Q \in K[X]\backslash(X-a)$. Comme $\frac{1}{Q}$ est inversible dans $K[X]_{(X-a)}$ d'inverse $\frac{Q}{1}$, on a $g(\frac{1}{Q}) = g(\frac{Q}{1})^{-1} = f(Q)^{-1}$ d'après le a. D'où

$$g(\tfrac{P}{Q}) = g(\tfrac{P}{1} \cdot \tfrac{1}{Q}) = g(\tfrac{P}{1}) \cdot g(\tfrac{1}{Q}) = f(P)f(Q)^{-1}.$$

c. Soit $\frac{P}{Q} \in A$, i.e., $P, Q \in K[X]$, $Q \neq 0$ et $\frac{P}{Q} \in A \subseteq K(X)$. On peut supposer P et Q premiers entre eux. Il existe alors $U, V \in K[X]$ tels que $UP + VQ = 1$ dans $K[X]$. On a alors

$$\tfrac{1}{Q} = \tfrac{UP+VQ}{Q} = U\tfrac{P}{Q} + V \in A.$$

Par conséquent, Q est inversible dans A. En particulier, $h(Q)$ est inversible dans K, c-à-d, $h(Q) \neq 0$. Mais $h(Q) = f(Q) = Q(a)$. Donc $Q(a) \neq 0$, i.e., Q n'est pas divisible par $X - a$. Par conséquent, $\frac{P}{Q} \in K[X]_{(X-a)}$.

4. Soit $f\colon \mathbb{Z} \to A$ l'unique morphisme de $\mathbb{Z}$ dans A. Par définition de la caractéristique, $\ker(f) = n\mathbb{Z}$. Soit $\pi\colon A \to A_{\text{red}}$ le passage au quotient. Rappelons que $\ker(\pi)$ est égal à $\text{Nil}(A)$, l'idéal des nilpotents de A. Pour montrer que la caractéristique de A_{red} est égale à m, il faut montrer que $\ker(\pi \circ f) = m\mathbb{Z}$.

Montrons l'inclusion $\ker(\pi \circ f) \supseteq m\mathbb{Z}$ en montrant que $m \in \ker(\pi \circ f)$. Evidemment, il existe $e \in \mathbb{N}$ tel que m^e soit divisible par n. (Il suffit de prendre $e = \sup\{e_i \mid i = 1, \ldots, g\}$.) On a alors $0 = f(m^e) = f(m)^e$ dans A, i.e., $f(m)$ est un nilpotent de A. Par conséquent, $(\pi \circ f)(m) = \pi(f(m)) = 0$.

Pour montrer l'inclusion $\ker(\pi \circ f) \subseteq m\mathbb{Z}$, soit $k \in \mathbb{Z}$ tel que $(\pi \circ f)(k) = 0$ dans A_{red}. Comme $\pi\colon A \to A_{\text{red}}$ est le quotient de A par $\text{Nil}(A)$, $f(k)$ est nilpotent dans A. Il existe alors $e \in \mathbb{N}$ tel que $f(k)^e = 0$. On a alors $k^e \in \ker(f)$ ce qui implique que n divise k^e. En particulier, tout nombre premier p divisant n divise k, donc m divise k. Par conséquent, $k \in m\mathbb{Z}$.