Anneaux et arithmétique

Examen terminal – Session 1
Corrigé

Exercice 1

Soit A, B deux anneaux unitaires et soit $f : A \to B$ un morphisme d'anneaux unitaires. Soit $I \subset A$ un idéal bilatère contenu dans $\ker f$. On note π la projection canonique de A dans A/I. Alors il existe un morphisme d'anneaux unitaires $\tilde{f} : A/I \to B$ tel que $f = \tilde{f} \circ \pi$. De plus, si f est surjectif, $\tilde{f}$ l'est aussi, et si $I = \ker f$, alors $\tilde{f}$ est injectif.

Exercice 2

1. **VRAI**
   C'est le cas pour tout anneau n'ayant pas d'éléments nilpotents non triviaux, par exemple un anneau intègre comme $\mathbf{Z}$. Pour un exemple d'anneau ayant un nombre fini non nul d'éléments nilpotents, on peut citer $\mathbf{Z}/4\mathbf{Z}$ dont le seul élément nilpotent non trivial est $\bar{2}$.
2. **FAUX**
   Dans un anneau local, il y a un unique idéal maximal, qui est l'ensemble des éléments non inversibles. Par exemple, l'anneau des séries formelles $\mathbf{R}[[X]]$ possède comme unique idéal maximal (X).
3. **VRAI**
   D'après le théorème de Lagrange, on a pour tout $x \in k^\times$, $x^{q-1} = 1$. En multipliant par x, on obtient l'identité $x^q = x$, qui reste vraie lorsque $x = 0$.
4. **VRAI**
   On considère la composée de l'évaluation en 0 $\mathbf{Z}[X, Y] \to \mathbf{Z}[X]$ et de la projection canonique $\mathbf{Z}[X] \to (\mathbf{Z}/2\mathbf{Z})[X]$. L'image $\bar{P}$ de P par cette projection est $X^4 + X + 1$, qui est irréductible dans $(\mathbf{Z}/2\mathbf{Z})[X]$. En effet, s'il était réductible, il aurait un diviseur irréductible Q de degré 1 ou 2, et Q diviserait $X^4 + X$ qui est premier avec $\bar{P}$. Cela montre que P est irréductible, car si P s'écrivait $P = AB$ avec A, B non constants, alors $\bar{P} = \bar{A}\bar{B}$. Comme $\deg \bar{P} = \deg P$, les polynômes $\bar{A}$ et $\bar{B}$ seraient non constants et $\bar{P}$ serait réductible, ce qui n'est pas.
5. **VRAI**
   Soit $x, y \in A$, on a alors $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + y + xy + yx$, d'où $xy + yx = 0$. Par ailleurs, on a $1 + xy = 1 + 2xy + xy$, d'où $2xy = 0$. Ainsi, $xy - yx = 0$, donc A est commutatif.

Exercice 3

1. La fonction constante égale à 1 est de classe $\mathcal{C}^\infty$, et la différence et le produit de deux fonctions $\mathcal{C}^\infty$ le sont également, donc A est un sous-anneau unitaire de $\mathcal{F}(\mathbf{R}, \mathbf{R})$.
2. Considérons l'application $\varepsilon : \left| \begin{array}{ccc} A & \to & \mathbf{R} \\ f & \mapsto & f(0) \end{array} \right.$. Cette application d'évaluation est clairement un morphisme d'anneaux surjectif (la fonction constante égale à c, qui est dans A, a pour image par ce morphisme le nombre réel c). Par définition de $\mathfrak{M}$, on a $\mathfrak{M} = \ker \varepsilon$, ce qui montre que $\mathfrak{M}$ est un idéal de A. De plus, ε induit un isomorphisme $A/\mathfrak{M} \to \mathbf{R}$. En particulier, $A/\mathfrak{M}$ est un corps, et donc l'idéal $\mathfrak{M}$ est maximal.
3. Considérons l'application $\varepsilon_\infty : \left| \begin{array}{ccc} A & \to & \mathbf{R}[[X]] \\ f & \mapsto & \sum_{n \geq 0} f^{(n)}(0) X^n \end{array} \right.$. Montrons d'abord qu'il s'agit d'un morphisme d'anneaux. Il est déjà clair que c'est un morphisme de groupes, et que $\varepsilon_\infty(1) = 1$. Il nous reste à vérifier que ε_∞ respecte le produit. Cela découle de la règle de Leibniz et de la formule de multiplication des séries formelles. Par définition, $\mathfrak{P} = \ker \varepsilon_\infty$, donc $\mathfrak{P}$ est un idéal de A. De plus $A/\mathfrak{P}$ s'identifie *via* ε_∞ à un sous-anneau de $\mathbf{R}[[X]]$, qui est intègre, donc $A/\mathfrak{P}$ est intègre, et $\mathfrak{P}$ est premier. On peut en fait montrer que ε_∞ est surjectif : ce résultat est connu sous le nom de théorème de Borel.

Exercice 4

1. Il est clair que $\ker \varphi \supset (Z - XY, Y^2 - X^3)$. Soit $P \in \ker \varphi$. Effectuons la division euclidienne de P par le polynôme unitaire en la variable Z, $Z - XY$. On a $P = A(Z - XY) + B$, avec B de degré ≤ 0 en Z. Le polynôme B ne dépend donc que des variables X et Y. On effectue la division euclidienne de B par le polynôme unitaire en Y, $Y^2 - X^3$. On a alors
$$P = A(Z - XY) + C(Y^2 - X^3) + R,$$
avec $R \in k[X, Y]$, de degré au plus 1 en Y. Ecrivons $R(X, Y) = U(X)Y + V(X)$, avec $U, V \in k[X]$. En appliquant φ, on trouve que $U(t^2)t^3 + V(t^2) = 0$. Notons u et v les valuations respectives de U et V, on a donc $2u + 3 = 2v$. Si U et V sont non nuls, cela est impossible car alors u et v sont entiers. On a donc $U = V = 0$, et $P \in (Z - XY, Y^2 - X^3)$.
2. Soit $f \in \mathrm{Hom}_k(A, k)$. On note x, y, z les classes respectives de X, Y, Z dans A : le morphisme f est entièrement déterminé par ses valeurs en x, y, z. Si $f(x) = 0$, alors $f(x)^3 = f(x^3) = f(y^2) = f(y)^2 = 0$, donc $f(y) = 0$, et $f(z) = f(x)f(y) = 0$. On a alors $f = 0$. Si $f(x) \neq 0$, posons $t = f(y)/f(x)$. On a alors $(f(x), f(y), f(z)) = (t^3, t^2, t^5)$. Cela nous définit donc une application $\mathrm{Hom}_k(A, k) \to \mathcal{C}$ (bien définie

également lorsque $f(x) = 0$). Cette application est injective du fait que f est déterminé par ses valeurs en x, y, z, et surjective car pour tout $t \in k$, il existe un unique morphisme de k-algèbres $k[X,Y,Z] \to k$ envoyant (X,Y,Z) sur (t^2, t^3, t^5) : c'est la composée de φ et de l'évaluation en t. Ce morphisme passe au quotient car $A = k[X,Y,Z]/\ker\varphi$, et l'élément de $\mathrm{Hom}_k(A,k)$ correspondant a bien pour image (t^2, t^3, t^5) par l'application $\mathrm{Hom}_k(A,k) \to \mathcal{C}$. Ainsi, $\mathrm{Hom}_k(A,k)$ est en bijection avec $\mathcal{C}$.

3. Le morphisme φ induit un morphisme injectif $A \to k[T]$. Comme $k[T]$ est intègre, A aussi. Ce morphisme se prolonge en un morphisme injectif (noté $\tilde{\varphi}$) $\mathrm{Frac}A \to k(T)$. De plus $T = \varphi(Y)/\varphi(X)$, donc $\tilde{\varphi}$ est surjectif, et $\mathrm{Frac}A$ est isomorphe à $k(T)$.
4. Dans A, on a $x^3 = y^2$. Les éléments x et y sont irréductibles dans A et non associés, donc x^3 admet deux factorisations non équivalentes dans A : A n'est pas factoriel.

Exercice 5

1. (a) Un inverse (au sens classique) est un inverse ponctuel, et 0 admet toujours 0 comme inverse ponctuel. Ainsi, dans un corps, tout élément admet un inverse ponctuel.
   (b) Si B est un corps, $B \backslash (\{0\} \cup B^\times) = \emptyset$, donc tout élément de $B \backslash (\{0\} \cup B^\times) = \emptyset$ n'a pas d'inverse ponctuel.
2. (a) Soit a inversible. Alors a^{-1} est clairement inverse ponctuel de a. De plus, si a' est un inverse ponctuel de a, on a $a^{-1}a^2a' = 1$ donc $aa' = 1$, et donc $a' = a^{-1}$.
   (b) Soit a' un inverse ponctuel de a, $(aa')^2 = a^2(a')^2 = aa'$. Donc aa' est idempotent. On suppose que $a \in A \backslash (\{0\} \cup A^\times)$, alors $a(aa' - 1) = 0$, alors si A était intègre, on aurait $a = 0$ ou $aa' = 1$, or ces deux possibilités sont exclues. Donc A n'est pas intègre.
   (c) On a $(1 - aa' + a')(1 - aa' + a) = 1 - aa' + a - aa' + (aa')^2 - a^2a' + a' - a(a')^2 + aa' = 1$, donc $1 - aa' + a$ est inversible dans A.
   (d) On a $(ab)^2a'b' = a^2a'b^2b' = ab$, et $ab(a'b')^2 = a'b'$, donc $a'b'$ est inverse ponctuel de ab dans A.
3. Soit $a \in A$, et notons a', a'' des inverses ponctuels de a dans A. On a $a' = (a')^2a = (a')^2(a^2a'') = aa'a''$. On a donc également $a'' = aa'a''$, d'où $a' = a''$, et l'unicité de l'inverse ponctuel de a.
4. Supposons que tout élément de l'anneau A possède un inverse ponctuel. Soit $\mathfrak{P}$ un idéal premier de A, et soit $a \in \mathfrak{P}$ et a' un inverse ponctuel de a dans A. Alors $aa' \in \mathfrak{P}$, donc $1 - aa' \in A \setminus \mathfrak{P}$ (sinon on aurait $1 \in \mathfrak{P}$), donc $1 - aa' \in A_{\mathfrak{P}}^\times$. Par ailleurs, $a(1 - aa') = 0$, donc $a = 0$ dans $A_{\mathfrak{P}}$. Soit $x \in A_{\mathfrak{P}}$ non nul, on écrit $x = \frac{a}{s}$ avec $s \notin \mathfrak{P}$. On a $a \notin \mathfrak{P}$ sinon $x = 0$. Ainsi, $y = \frac{s}{a} \in A_{\mathfrak{P}}$ est un inverse de x. Donc $A_{\mathfrak{P}}$ est un corps.

5. Montrons que les assertions suivantes sont équivalentes :
$(a) \Rightarrow (b)$: Soit a' un inverse ponctuel de a, alors $a^2a' = a \in a^2A$.
$(b) \Rightarrow (c)$: Soit $\varphi : A \to A/(a) \times A_a$ envoyant $x \in A$ sur $(\bar{x}, \frac{x}{1})$. Commençons par examiner le noyau de φ : soit $x \in \ker \varphi$, alors $x \in (a)$ et $x \sim 0$ dans A_a. Cette deuxième condition signifie encore qu'il existe $s \in \mathbf{N}$ tel que $a^n x = 0$. Supposons maintenant que (b) soit vérifiée, et soit $a' \in A$ tel que $a = a^2a'$. Soit $x \in \ker \varphi$ et soit $n \in \mathbf{N}$ minimal tel que $a^n x = 0$, et supposons $n \geq 1$. Comme $x \in (a)$, écrivons $x = az$. Alors $a^{n+1}z = 0$, donc $a^{n-1}a^2z = 0$, d'où $a^{n-1}az = 0$ (en multipliant par a'). Cela contredit la minimalité de n, donc $n = 0$. Ainsi, $x = 0$ et φ est injectif. Enfin, $\varphi(1 - aa') = (1, 0)$ car $a(1 - aa') = 0$, donc $\varphi(aa') = (0, 1)$, et donc φ est surjectif.
$(c) \Rightarrow (a)$: Soit $z \in A$ un antécédent de $(0, 1)$ par le morphisme φ. On écrit $z = aa'$. On a alors $aa' = 1$ dans A_a, c'est-à-dire qu'il existe $n \in \mathbf{N}$ tel que $a^n(1 - aa') = 0$. Supposons n minimal et $n \geq 2$, alors $\varphi(a^{n-1}(1 - aa')) = (0, 0)$. Par injectivité, $a^{n-1}(1 - aa') = 0$, ce qui contredit la minimalité de n. Ainsi, $n \in \{0, 1\}$. Si $n = 0$, alors a est inversible d'inverse a', et en particulier admet comme pseudo-inverse a'. Sinon, $n = 1$ et $a^2a' = a$. Soit alors b un antécédent de $(0, a'/1)$ par φ, on a encore $a^2b = a$ et $\varphi(b^2a) = (0, a'/1) = \varphi(b)$, donc $b^2a = b$. Ainsi, b est un pseudo-inverse de a.