Partiel

Corrigé

Exercice 1 : (3 pts) Soit $f : A \to B$ un morphisme d'anneaux.

1. Montrer que si J est un idéal de B, alors son image réciproque $f^{-1}[J]$ est un idéal de A.
2. Montrer que si f est surjective et I est un idéal de A, alors son image directe $f[I]$ est un idéal de B.
3. Donner un exemple de f non-surjectif et I idéal dans A tel que $f[I]$ n'est pas un idéal dans B.

Solution.

1. On a $f(0) \in I$, donc $0 \in f^{-1}[J]$. Soient $a, b \in f^{-1}[J]$, donc $f(a), f(b) \in I$. Alors $f(a \pm b) = f(a) \pm f(b) \in I$ et $a \pm b \in f^{-1}[J]$. De plus, pour $c \in A$ on a $f(ca) = f(c)f(a) \in I$ et $c \in f^{-1}[J]$. Ainsi $f^{-1}[J]$ est un idéal de A.
2. On a $0 \in I$ et $f(0) = 0$, d'où $0 \in f[I]$. Soient $a, b \in f[I]$, donc il y a $a', b' \in I$ avec $f(a') = a$ et $f(b') = b$. Alors $a' \pm b' \in I$ et $f(a' \pm b') = f(a') \pm f(b') = a \pm b \in f[I]$. De plus, pour $c \in B$ il y a $c' \in A$ avec $f(c') = c$ par surjectivité, et $c'a' \in I$. Alors $f(c'a') = f(c')f(a') = ca \in f[IJ]$. Ainsi $f[I]$ est un idéal de B.
3. In prend $A = I = \mathbb{Z}$, $B = \mathbb{Q}$ et $f = \mathrm{id}$. Alors I est trivialement un idéal dans A, mais $f[I] = f[\mathbb{Z}] = \mathbb{Z}$ n'est pas un idéal dans $B = \mathbb{Q}$ ($\mathbb{Z}$ n'est pas clos par multiplication par $1/2 \in \mathbb{Q}$).

Exercice 2 : (5 pts) Soit $n \in \mathbb{N}$ et $a_1, \dots, a_n \in \mathbb{Z}$ deux à deux distincts. Soit $P = (X - a_1) \cdots (X - a_n) + 1 \in \mathbb{Z}[X]$.

1. Supposons n impair. Montrer que P est irréductible dans $\mathbb{Z}[X]$.
2. Que dire de l'irréductibilité de P dans $\mathbb{Z}[X]$ si n est pair ?

Solution.

1. Pour $n = 0$ on a $P = 1$, ce qui est irréductible dans $\mathbb{Z}$. On suppose donc que $n \geq 1$.
   Pour une contradiction, supposons que $P = QR$ avec $Q, R \in \mathbb{Z}[X]$ non-inversible. Alors $Q(a_i)R(a_i) = P(a_i) = 1$ pour $i = 1, \dots, n$, et $Q(a_i) = R(a_i) = \pm 1$. Or $c(P) = 1$, d'où $\deg Q, \deg R < \deg P = n$. Mais $Q - R$ a n racies $a_1, \dots, a_n$, d'où $Q = R$ et $n = \deg P = 2 \deg Q$ est pair, une contradiction.
2. Tout peut arriver. Par exemple $(x-1)(x-3)+1 = (x-2)^2$ n'est pas irréductible, et $(x-1)(x-2)+1 = x^2 - 3x + 3$ est irréductible.

Exercice 3 : (5 pts)

1. Pour tout $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ avec $a_n \neq 0$, on note $P^* = \sum_{i=0}^{n} a_{n-i} X^i$.
   (a) Montrer que $P(X) = X^n P^*(1/X)$.
   (b) Montrer que si P est irréductible dans $\mathbb{Z}[X]$, alors P^* est irréducible dans $\mathbb{Z}[X]$.
2. Montrer que le polynôme $2X^5 - 4X^2 - 3$ est irréductible dans $\mathbb{Z}[X]$.

Solution.

1. (a) $X^n P^*(1/X) = X^n \displaystyle\sum_{i=0}^{n} a_{n-i}(1/X)^i = \sum_{i=0}^{n} a_{n-i} X^{n-i} = \sum_{i=0}^{n} a_i X^i = P(X)$.
   (b) Supposons que $P^* = QR$ avec $Q, R \in \mathbb{Z}[X]$ non-inversibles. Soit $k = \deg(Q)$ et $m = \deg(R)$. Alors $k + m = n$. On a

$$P(X) = X^n P^*(1/X) = X^n Q(1/X) R(1/X) = X^k Q(1/X) X^m R(1/X) = Q^*(X) R^*(X),$$

   ce qui est une factorisation non triviale de P.
2. Soit $P = 2X^5 - 4X^2 - 3$. Alors $P^* = -3X^5 - 4X^3 + 2$. Alors 2 divise tous les coefficients de P^* sauf le coefficient dominant, et 2^2 ne divise pas le coefficient constant ; d'après le critère d'Eisenstein, P^* est irréductible sur $\mathbb{Z}$, et P aussi d'après 1.(b).

Exercice 4 : (6 pts) Soit $A = \mathbb{Z}[i\sqrt{2}]$.

1. Montrer que $N(a + i\sqrt{2}b) = a^2 + 2b^2$ est une norme sur A qui en fait un anneau euclidien.
2. Soit $(x, y) \in \mathbb{Z}^2$ une solution de l'équation diophantienne $y^3 - x^2 = 2$. Montrer que $x + i\sqrt{2}$ est un cube dans A. En déduire l'ensemble des solutions de l'équation.

Solution.

1. Pour $z \in A$ on a $N(z) = |z|^2$; la fonction N est donc multiplicative, et $N(z) \geq 1$ pour $z \neq 0$. Donc $N(ab) = N(a)\,N(b) \geq N(a)$ pour tout $a, b \in A^*$.
   Soient $a, b \in A$ avec $b \neq 0$. En regardant le réseau $\mathbb{Z} + i\sqrt{2}\mathbb{Z}$, on trouve $x, y \in \mathbb{Z}$ tels que
   $$|\frac{a}{b} - (x + iy\sqrt{2})| \leq \sqrt{3}/2.$$
   On pose $q = x + iy\sqrt{2} \in A$ et $r = a - bq \in A$. Alors
   $$N(r) = |a - bq|^2 \leq 3|b|^2/4 < N(b).$$
   Ainsi N est une norme euclidienne sur A, et A est un anneau euclidien.
2. Si (x, y) est une solution de $y^3 - x^2 = 2$, alors $y^3 = x^2 + 2 = (x + i\sqrt{2})(x - i\sqrt{2})$. Or, les seuls éléments inversibles de A sont ceux de norme égale à $N(1) = 1$, donc ± 1. Si $y = \prod_\ell a_\ell^{n_\ell}$ est la factorisation de y en facteurs premiers, alors $y^3 = \prod_\ell a_\ell^{3n_\ell}$; si on montre que $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entr'eux, ils ne peuvent avoir aucun facteur a_ℓ en commun. Ainsi chacun est une puissance cube.
   Notons que si x est pair, y doit être pair, mais alors $2 = y^3 - x^2$ est divisible par 4, une contradiction. Donc $x \equiv \pm 1 \mod 4$. On calcule le pgcd :
   $$\begin{aligned} x + i\sqrt{2} \wedge x - i\sqrt{2} &= x + i\sqrt{2} \wedge 2i\sqrt{2} \mid x + i\sqrt{2} \wedge 2i\sqrt{2} \cdot i\sqrt{2} \\ &= x + i\sqrt{2} \wedge 4 = \pm 1 + i\sqrt{2} \wedge 4 \mid (\pm 1 + i\sqrt{2}) \cdot (\pm 1 - i\sqrt{2}) \wedge 4 = 3 \wedge 4 = 1. \end{aligned}$$
   Il y a donc $a, b \in \mathbb{Z}$ avec
   $$x + i\sqrt{2} = (a + ib\sqrt{2})^3 = a^3 - 6ab^2 + i\sqrt{2}(3a^2b - 2b^3).$$
   Ainsi $(3a^2 - 2b^2)b = 1$ et $b = \pm 1$. Donc $3a^2 - 2b^2 = 3a^2 - 2 = \pm 1$ et $3a^2 \in \{3, 1\}$. Alors $3a^2 = 1$ est impossible, et $b = 1$. Enfin $a = \pm 1$, et $x = a^3 - 6ab^2 = \pm(1 - 6) = \pm 5$. Ceci donne $y^3 = 2 + x^2 = 2 + 25 = 27$ et $y = 3$. Les deux solutions sont $(5, 3)$ et $(-5, 3)$.

Exercice 5 : (6 pts) Un anneau est *artinien* s'il n'y a pas de chaîne infinie strictement descendante $A > I_1 > I_2 > \cdots$ d'idéaux. On cherche à montrer qu'un anneau artinien intègre non-trivial est un corps. Soit donc $A \neq \{0\}$ un anneau artinien intègre.
Attention, si on ne sait pas que A est unitaire, on rappelle que $(x) = \mathbb{Z}x + Ax$.

1. Montrer que si $e \in A$ satisfait $ea = a$ pour un $a \in A^*$, alors $ea = a$ pour tout $a \in A$. (Cela n'utilise pas que A est artinien.)
2. Pour $x \in A^*$ trouver des entiers $m < n$, $z \in \mathbb{Z}$ et $a \in A$ avec $x^m = (zx^{n-m} + ax^{n-m})x^m$. En déduire que A est unitaire.
3. Pour $x \in A^*$ montrer que x est inversible. Conclure que A est un corps.

Solution.

1. Soit $b \in A$. Alors $eab = ab$, d'où $0 = eab - ab = a(eb - b)$; puisque $a \neq 0$ on a $eb - b = 0$ et $eb = b$ par intégrité de A.
2. Soit $x \in A^*$. On considère la chaîne d'idéaux $(x) \geq (x^2) \geq (x^3) \geq \cdots$. Puisque A est artinien, il y a $m \in \mathbb{N}^*$ tel que $(x^m) = (x^{m+1})$. En particulier $x^m \in (x^{m+1}) = \mathbb{Z}x^{m+1} + Ax^{m+1}$, et il y a $z \in \mathbb{Z}$ et $a \in A$ avec $x^m = zx^{m+1} + ax^{m+1} = (zx + ax)x^m$. On pose $e = zx + ax \in A$. Par intégrité de A on a $x^m \neq 0$, donc e est unité d'après 1. et A est unitaire. (On a donc $n = m + 1$.)
3. Soit $x \in A^*$; comme ci-dessus il y a $m \in \mathbb{N}^*$ tel que $(x^m) = (x^{m+1})$ et $x^m \in (x^{m+1}) = Ax^{m+1}$. Il y a donc $a' \in A$ avec $x^m = a'x^{m+1}$, d'où $(a'x - e)x^m = 0$. Puisque $x^m \neq 0$ on a $a'x = e$ et x est inversible. Ainsi tout élément de A^* est inversible et A est un corps.