122. Anneaux principaux : indications de solutions

1. a) C'est vrai, et résulte immédiatement de la définition (noter d'ailleurs que l'anneau nul n'est pas un sous-anneau d'un anneau non nul, car le neutre pour la multiplication n'est pas le même !).

b) C'est faux, car un anneau intègre non principal (par exemple $\mathbf{C}[X, Y]$) est un sous-anneau de son corps des fractions, lequel est un anneau principal.

c) C'est vrai car soit $I = \{0\}$ (auquel cas c'est clair), soit $I = (p)$ avec p irréductible, auquel cas dans un anneau principal $A/(p)$ est un corps via le théorème de Bezout.

d) C'est vrai car on voit tout de suite que f induit un morphisme d'anneau injectif $A/f^{-1}(\wp) \to B/\wp$, ce qui montre que $A/f^{-1}(\wp)$ est isomorphe à un sous-anneau d'un anneau intègre, donc est intègre.

2. a) Immédiat en notant que a/d et b/d sont premiers entre eux (noter que comme A est intègre et a, b sont divisibles par d, a/d et b/d ont bien un sens).

b) Par récurrence sur n. C'est clair pour $n \leq 2$ avec l'hypothèse. Supposons le résultat vrai jusqu'à $n-1$. Soit $d = \text{pgcd}(a_1, ..., a_{n-1})$. Alors il existe u, v dans A avec $ud + va_n = 1$ car $\text{pgcd}(d, a_n) = 1$ par définition du pgcd. Ensuite, l'hypothèse de récurrence appliquée à $a_1/d, ..., a_{n-1}/d$ donne une décomposition

$$d = u_1 a_1 + ... + u_{n-1} a_{n-1}, \quad u_1, ..., u_{n-1} \in A,$$

d'où on déduit le résultat.

c) Si I est nul ou $I = A$, c'est clair. Sinon I contient un élément non nul et non inversible a, qu'on peut écrire

$$a = u. \prod_{i=1}^{r} p_i^{v_i(a)},$$

avec $u \in A^*$, $v_i(a) \in \mathbf{N}$, et les p_i irréductibles non associés deux à deux. Soit alors, pour chaque i, a_i un élément de I tel que $w_i := v_i(a_i)$ soit minimum parmi les $v_i(x)$ avec $x \in I$. Le pgcd de tous les éléments de I est alors

$$\prod_{i=1}^{r} p_i^{w_i},$$

qui est aussi le pgcd de $a, a_1, ..., a_r$.

d) Soient I un idéal de A et d le pgcd de tous les éléments de I. D'après c), c'est aussi le pgcd d'une famille finie $a_1, ..., a_r$ d'éléments de I. En appliquant b) à $a_1/d, ..., a_r/d$, on obtient que $d \in I$, d'où $(d) \subset I$. Par ailleurs $I \subset (d)$ par définition du pgcd de tous les éléments de I. Finalement I est bien principal.

3. a) Immédiat à partir des définitions.

b) On voit tout de suite que A est un sous-anneau de K. Si $s \in S$, alors il admet pour inverse $1/s$ dans A_S.

c) Soit J un idéal de A_S. Alors son image réciproque par le morphisme d'inclusion $A \to A_S$ est un idéal I de A. Comme $J \supset I$ et J est un idéal de A_S, on a $J \supset IA_S$, et en sens inverse tout élément $y = x/s$ de J avec $x \in A$ vérifie $x = s(x/s) \in J \cap A_S = A$, ce qui montre que $x \in A$ et $y \in IA_S$. Finalement on a bien $J = IA_S$. Si J est premier, alors I est premier (image réciproque d'un idéal premier par un morphisme d'anneaux, cf. exercice 1) et ne rencontre pas S (sinon J contiendrait un inversible et serait égal à A_S). En sens inverse, si I est premier et ne rencontre pas S, alors $1 \notin J = IA_S$ et on voit tout de suite que si $(x/s)(x'/s') \in J$ avec s, s' dans S et x, x' dans A, alors $xx' \in J \cap A = I$, donc $x \in I$ ou $x' \in I$, ce qui montre que J est premier. Finalement IA_S est premier ssi I est premier et ne rencontre pas S.

d) L'anneau A_S est intègre, et c) montre immédiatement que tout idéal de A_S est principal. Donc A_S est principal. L'anneau des décimaux est le cas particulier où $A = \mathbf{Z}$ et S est l'ensemble des $10^k, k \in \mathbf{N}$. La même assertion est vraie pour euclidien, mais c'est plus difficile.

e) Si $S = A - \wp$, les idéaux premiers de A_S sont les idéaux de la forme IA_S, où I est un idéal premier de A ne rencontrant pas S, i.e. inclus dans $\wp$. Quand $A = \mathbf{Z}$, on obtient pour chaque nombre premier p l'anneau des x/y avec $x \in \mathbf{Z}$ et y non divisible par p. Son complété pour la topologie associée à la valuation p-adique est l'*anneau des entiers p-adiques* $\mathbf{Z}_p$.

4. Via les deux décompositions différentes en irréductibles

$$9 = 3.3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

on va montrer que 9 et $3(2+i\sqrt{5})$ n'ont pas de pgcd dans A. On voit déjà que 3 est un diviseur commun, donc si d était un pgcd, alors $d/3$ serait un pgcd de 3 et $2+i\sqrt{5}$; or, ces deux éléments sont irréductibles non associés, et donc premiers entre eux. Ainsi on aurait $d = 3$ (à association près), mais comme $2 + i\sqrt{5}$ est aussi un diviseur commun de 9 et $3(2 + i\sqrt{5})$, cela impliquerait que $2 + i\sqrt{5}$ divise 3, ce qui n'est pas le cas.

5. a) Les zéros d'une fonction holomorphe non nulle sont isolés. On en déduit immédiatement que le produit de deux fonctions holomorphes non nulles est non nulle, et donc que l'anneau non nul H est intègre. Son corps des fractions est par définition le corps des fonctions méromorphes sur $\mathbf{C}$.

b) Si f est holomorphe et ne s'annule pas, on sait que $1/f$ est holomorphe et donc $f \in H^*$. En sens inverse s'il existe g tel que $fg = 1$, il est clair que f ne s'annule pas.

Si maintenant f est irréductible, elle n'est pas inversible, donc possède un zéro a. On sait alors que la fonction g définie par $g(z) = f(z)/(z - a)$ est encore dans H, et comme $h : z \mapsto (z - a)$ n'est pas inversible, la fonction g doit être inversible ce qui montre que a est le seul zéro de f et qu'il est simple. En sens inverse, si f admet a comme unique zéro et ce zéro est simple, alors si $f = f_1 f_2$ avec f_1, f_2 dans H, l'une des fonctions f_1, f_2 ne s'annule pas donc est dans H^*, ce qui montre que f est irréductible. On a en fait montré qu'un système de représentants irréductibles est constitué des fonctions de la forme $z \mapsto (z - a)$ avec $a \in \mathbf{C}$.

c) Soit une fonction holomorphe non nulle possédant une infinité de zéros, par exemple $z \mapsto \sin z$. Alors d'après b), elle ne peut pas s'écrire comme produit d'un inversible et d'un nombre fini d'irréductibles, donc H n'est ni factoriel ni noethérien. On peut par contre montrer (plus difficile) que H vérifie le théorème de Bezout, ou encore que tout idéal *de type fini* de H est principal.

6. Par hypothèse on peut écrire $1 = a_1 + b = a_2 + c$ avec $a_1 \in I_1$, $a_2 \in I_2$, et $b, c \in J$. En faisant le produit, on obtient $1 = a_1 a_2 + (a_1 c + b a_2 + bc)$ avec $a_1 a_2 \in I_1 I_2$ et $(c + b a_2 + bc) \in J$, ce qui montre que $I_1 I_2$ est encore étranger avec J.

b) L'idéal (p) est premier non nul car A est factoriel et p irréductible, il est donc maximal. Comme p ne divise pas a, l'idéal (a, p) contient strictement (p), il est donc égal à A, ce qui montre que (p) est étranger avec (a).

c) Écrivons la décomposition de a :

$$a = up_1 ... p_r,$$

avec $u \in A^*$ et les p_i irréductibles. Comme a et b sont premiers entre eux, p_i ne divise pas b, et d'après b), (p_i) est étranger avec (b). D'après a) et par une récurrence facile, $(p_1)...(p_r) = (a)$ est étranger avec b. On peut donc écrire $a = va + wb$ avec v, w dans A. L'exercice 2 de cette feuille montre alors que A est principal, car il est factoriel et vérifie le théorème de Bezout. Noter que A n'avait pas été supposé noethérien au départ (il existe des anneaux intègres non noethériens tels que tout idéal premier non nul soit maximal, par exemple la fermeture intégrale de l'anneau $\mathbf{Z}_p$ des entiers p-adique dans la clôture algébrique $\overline{\mathbf{Q}_p}$ de son corps des fractions $\mathbf{Q}_p$).

7. a) Soient a, b dans A avec $b \neq 0$, on cherche à écrire $a = bq + r$ avec $w(r) < w(b)$ ou $r = 0$. On peut supposer que b ne divise pas a. Par définition de w, on peut écrire $w(b) = v(bs)$ avec $s \in A$ tel que $v(bs)$ soit minimal. On effectue alors la division euclidienne de as par bs pour v, ce qui donne $as = bsq+t$ avec $q, t \in A$ et $v(t) < v(bs)$ (en effet on ne peut avoir $t = 0$, sinon b diviserait a). En particulier s divise t et on pose $t = rs$. Alors $a = bq + r$ et

$$w(r) \leq v(rs) < v(bs) = w(b).$$

b) Par définition de w, on a $w(x) \leq v(xys)$ pour tout s de A, d'où, en prenant le min sur s, $w(x) \leq w(xy)$. Autrement dit, si x divise z, alors $v(x) \leq v(z)$. En échangeant les rôles de x et z, on voit $w(x) = w(z)$ si x et z sont associés, comme on voulait.

c) D'après b), on a $w(y) = w(1.y) \geq w(1)$ pour tout y de A, ce qui montre que $w(1) = m$, et donc $w(u) = 1$ si $u \in A^*$ puisqu'alors u est associé à 1. Réciproquement, si $w(b) = m$, on effectue la division euclidienne de 1 par b pour w, ce qui donne $1 = bq + r$, avec forcément $r = 0$ (sinon on aurait $w(r) < w(b)$, ce qui contredit la minimalité de $w(b)$), ce qui montre que $1 = bq$, et donc $b \in A^*$.