Anneaux factoriels et non factoriels

Vous trouverez des détails sur certains des points qui suivent (mais pas tous) dans le Cours d'Algèbre de Daniel Perrin.

1 Quelques rappels sur les anneaux factoriels

Cadre général. L'arithmétique, c'est l'étude des relations de divisibilité. Le cadre habituel pour cette étude est celui des anneaux commutatifs, unitaires. On s'intéresse la plupart du temps à des anneaux intègres, à la fois car la plupart des exemples historiques qui ont motivé les mathématiciens (dont les anneaux d'entiers dans les corps de nombres) sont des anneaux intègres, et aussi car l'hypothèse d'intégrité est très commode, voire souvent nécessaire pour mener à bien les raisonnements que l'on a en vue. En résumé, disons qu'on considère, dans cette feuille au moins, la famille $\mathcal{F}$ des anneaux commutatifs unitaires et intègres. Il faut tout de même noter qu'on est souvent amené à réduire modulo un idéal et que dans ce cas, on tombe sur un anneau qui possède toutes les caractéristiques précédentes, sauf peut-être l'intégrité.

Anneaux factoriels. Dans la famille $\mathcal{F}$, les anneaux les plus sympathiques pour faire de l'arithmétique sont les anneaux *factoriels*, qui sont par définition les anneaux A tels que :

(I) A est intègre,
(E) tout élément non nul s'écrit comme un produit $a = up_1 \dots p_r$ avec u inversible et les p_i irréductibles (non distincts)
(U) une décomposition comme dans (E) est unique, à permutation près des facteurs et aux éléments inversibles près.

On notera qu'un anneau factoriel n'est pas nécessairement noethérien (par exemple, l'anneau $\mathbb{Q}[X_1, X_2, X_3, \dots]$ de polynômes en une infinité de variables est factoriel non noethérien). Néanmoins, les anneaux que l'on étudie en arithmétique sont presque tout le temps noethériens (extensions de $\mathbb{Z}$ ou d'un corps engendrées par un nombre fini d'éléments). Or, un anneau noethérien vérifie toujours la condition (E). Finalement, retenons que la propriété véritablement distinctive des anneaux factoriels est la validité de la condition (U).

Pgcd et ppcm. Dans cette note constituée d'exercices, on s'intéresse en particulier au comportement des pgcd et ppcm, et notamment à leur (non-)existence éventuelle. Rappelons que dans un anneau intègre A, l'ensemble $A \setminus \{0\}$ des éléments non nuls est un monoïde multiplicatif, l'ensemble A^* des inversibles est un sous-monoïde qui est un groupe et qui donne naissance à la relation d'*association* : a et b sont associés s'il existe $u \in A^*$ tel que $a = ub$. On note parfois $a \sim b$. La relation de divisibilité :

$$a \geq b \quad \text{ssi} \quad a \,|\, b \ ,$$

est une relation d'ordre sur $A \setminus \{0\}$, ou sur son quotient $(A \setminus \{0\})/\sim$, compatible à la structure de monoïde. Si deux éléments a et b de $A \setminus \{0\}$ possèdent un majorant, on l'appelle « un » pgcd (dans $A \setminus \{0\}$) ou « le » pgcd (dans $(A \setminus \{0\})/\sim$). S'ils possèdent un minorant, on l'appelle

« un » ou « le » ppcm. (Attention au fait que si l'on choisit la convention inverse pour la relation d'ordre, c'est-à-dire si l'on écrit que a divise b se note $a \leq b$ au lieu de $a \geq b$, alors les notions de sup et d'inf sont renversées.)

2 Exercices

Dans chaque exercice, on s'autorise à utiliser le résultat de ceux qui le précèdent, et il est donc plus adapté de les faire dans l'ordre.

Exercice 1 Soit A un anneau intègre et a, b, x non nuls dans A. Montrez que si xa et xb possèdent un pgcd, alors a et b possèdent un pgcd et on a la formule $\text{pgcd}(xa, xb) = x\text{pgcd}(a, b)$.

Remarque : il n'est pas toujours vrai que si a et b possèdent un pgcd, alors xa et xb en possèdent un. On donnera un contre-exemple dans l'exercice 4.

Exercice 2 Soit A un anneau intègre noethérien. Montrez que les conditions suivantes sont équivalentes :
(i) A est factoriel,
(ii) tout couple d'éléments de A possède un pgcd.

Exercice 3 Soient A un anneau intègre et a, b deux éléments de A. Montrez que si a et b possèdent un ppcm m, alors ils possèdent un pgcd d et on a la formule $ab = md$.

Remarque : il n'est pas toujours vrai que si a et b possèdent un pgcd, ils possèdent un ppcm. On donnera un contre-exemple dans l'exercice 4.

Terminons avec un exemple d'anneau (intègre, noethérien) non factoriel. Pour fabriquer cet exemple, on suit une idée simplissime et extrêment importante qui utilise à fond la possibilité donnée par les quotients d'anneaux de polynômes de construire des exemples d'anneaux possédant un certain nombre fixé (fini) d'éléments satisfaisant un certain nombre (fini) de relations données. Précisément, l'idée est que pour trouver un anneau non factoriel, on va chercher un anneau contenant un élément qui possède deux décompositions en irréductibles distinctes de la forme $xy = zt$ où x, y, z, t sont des irréductibles tous distincts. On peut construire un tel anneau de manière « universelle » en considérant l'anneau de l'exercice.

Exercice 4 On considère l'anneau $A = k[X, Y, Z, T]/(XY - ZT)$, quotient d'un anneau de polynômes en quatre indéterminées. On note x, y, z, t les images de X, Y, Z, T dans A.

(0) Soit R un anneau intègre et $R[X, 1/X]$ le sous-ensemble du corps des fractions de $R[X]$ composé des fractions de la forme $P(X)/X^n$ avec $n \geq 0$ entier. Montrez que $R[X, 1/X]$ est un anneau. Montrez que tout élément de $R[X, 1/X]$ s'écrit d'une manière unique sous la forme $\sum_{i \in I} r_i X^i$ avec I un sous-ensemble *fini* de $\mathbb{Z}$ et $r_i \in R$ pour tout $i \in I$.
*On appelle $R[X, 1/X]$ l'*anneau des polynômes de Laurent en X à coefficients dans R *; c'est une R-algèbre et la famille $\{X^i, i \in \mathbb{Z}\}$ est une base du R-module sous-jacent.*

(1) On considère l'anneau $R = k[z, t] \subset A$ isomorphe à $k[Z, T]$. Montrez que tout élément de A possède une écriture unique $a = a_0 + xa_1(x) + ya_2(y)$ où $a_0 \in R$, $a_1 \in R[x]$ et $a_2 \in R[y]$.

(2) Montrez que A est intègre en construisant une injection de A dans $B = k[Z, T][X, 1/X]$.

(3) Montrez que z et t sont des irréductibles de A. Indiquez pourquoi x et y le sont aussi.

(4) Justifiez qu'aucun de ces quatre irréductibles n'est multiple d'un autre ; en particulier, ils sont non associés deux à deux.

(5) Montrez que A n'est pas factoriel.

(6) Montrez que xz et xy n'ont pas de pgcd.

(7) Montrez que x et z ont un pgcd mais n'ont pas de ppcm (utiliser l'exercice 3).

3 Corrigés

Corrigé exercice 1. Supposons que xa et xb possèdent un pgcd et notons-le e. Comme x divise xa et xb, on a x divise e. Soit d tel que $e = xd$. Il suffit de montrer que d est un pgcd pour a et b pour résoudre l'exercice. D'abord, du fait que $e = xd$ divise xa et xb, on tire que d divise a et b. Ensuite, si d' divise a et b, alors xd' divise xa et xb, donc xd' divise $\mathrm{pgcd}(xa, xb) = e = xd$. Ainsi d' divise d, ce qui conclut la démonstration. □

Corrigé exercice 2. On sait que (i) implique (ii), et il faut donc prouver la réciproque. Supposons pour cela que A n'est pas factoriel, c'est-à-dire qu'il ne vérifie pas la condition (U). Alors il existe un élément $a \in A$ non nul qui possède deux décompositions en irréductibles distinctes : $a = up_1^{\alpha_1} \dots p_r^{\alpha_r} = vq_1^{\beta_1} \dots q_s^{\beta_s}$ (où l'on suppose que les α_i et les β_j sont > 0).

Notons $P = \{p_1, \dots, p_r\}$ et $Q = \{q_1, \dots, q_s\}$. Pour tout $a \in A$, notons $\mu(a)$ la plus petite des valeurs $\alpha_1 + \dots + \alpha_r$, prise parmi toutes les décompositions en irréductibles possibles $a = up_1^{\alpha_1} \dots p_r^{\alpha_r}$. Si on choisit a tel que $\mu(a)$ est minimal, on aura $P \cap Q = \emptyset$. En effet, sinon P et Q ont un élément commun, que l'on peut supposer être $p_1 = q_1$ quitte à renuméroter. Alors, en divisant par $p_1 = q_1$ de part et d'autre, on obtient un élément a' qui possède deux décompositions en irréductibles distinctes :

$$a' = up_1^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = vq_1^{\beta_1 - 1} \dots q_s^{\beta_s}$$

et $\mu(a') < \mu(a)$, en contradiction avec le choix de a.

On a donc un élément a décomposé de deux manières, comme ci-dessus, avec P et Q disjoints. Soit $b = p_1 q_1$. Si a et b possèdent un pgcd, alors en utilisant l'exercice 1 on trouve

$$\mathrm{pgcd}(a, b) = \mathrm{pgcd}(up_1^{\alpha_1} \dots p_r^{\alpha_r}, p_1 q_1) = p_1 \mathrm{pgcd}(up_1^{\alpha_1 - 1} \dots p_r^{\alpha_r}, q_1) = p_1$$

puisque q_1 ne divise aucun des p_i. Par ailleurs

$$\mathrm{pgcd}(a, b) = \mathrm{pgcd}(vq_1^{\beta_1} \dots q_s^{\beta_s}, p_1 q_1) = q_1 \mathrm{pgcd}(vq_1^{\beta_1 - 1} \dots q_s^{\beta_s}, p_1) = q_1 \ .$$

On obtient $p_1 = q_1$ ce qui n'est pas possible. Donc a et b ne possèdent pas de pgcd, ce que l'on voulait démontrer. □

Corrigé exercice 3. Notons m le ppcm de a et b. Comme ab est un multiple commun de a et b, c'est un multiple de m : il existe d tel que $ab = md$. Montrons que d est un pgcd pour a et b.

Comme m est multiple de a et b, il existe u, v tels que $m = ua = vb$. On en déduit que $ab = uad$ donc $b = ud$, et $ab = vbd$ donc $a = vd$. Ainsi d est diviseur commun de a et b.

Soit e un diviseur quelconque de a et b. Alors il existe α, β tels que $a = e\alpha$ et $b = e\beta$, donc $e\alpha\beta$ qui vaut à la fois $a\beta$ et $b\alpha$ est un multiple commun de a et b. Ainsi, il existe f tel que $e\alpha\beta = mf$. Alors, $b\alpha = e\alpha\beta = mf = vbf$ donc $\alpha = vf$. On en tire $vd = a = e\alpha = evf$ donc $d = ef$, i.e. e divise d et d est le pgcd de a et b. □

Précédons la correction de l'exercice 4 par un commentaire sur les calculs dans les anneaux quotients. Comme toujours avec les quotients (quotient X/R d'un ensemble par une relation d'équivalence, quotient G/H d'un groupe par un sous-groupe distingué ou non, quotient A/I d'un anneau par un idéal), la plupart du temps la seule manière de faire des calculs avec les éléments d'un quotient est d'en choisir des préimages (dans X, resp. G, resp. A) et de raisonner « en haut » mais évidemment modulo (R, H, I). Avec un anneau A, une seconde possibilité se présente parfois : il s'agit grosso modo d'utiliser un analogue *ad hoc* de la division euclidienne pour obtenir une écriture *unique* agréable pour les éléments de A. L'exemple modèle est celui des quotients d'anneaux de polynôme en une variable : dans $A = k[X]/(P)$ avec P unitaire de degré n, par division euclidienne tout élément de A s'écrit de manière unique sous la forme d'un polynôme de degré $\leq n-1$ en x, l'image de X dans A.

Corrigé exercice 4. (0) Ceci est laissé à la lectrice.

(1) Choisissons un polynôme $P \in k[X, Y, Z, T]$ d'image $a \in A$, et raisonnons modulo $(XY - ZT)$. On écrit P comme polynôme en X et Y à coefficients dans $k[Z, T]$. Il est donc somme de monômes X^iY^j, et à chaque fois que $i \geq 1$ et $j \geq 1$, on peut mettre en facteur XY dans ce monôme et le remplacer par ZT, vu comme une « constante » de notre sous-anneau $k[Z, T]$. En itérant ce procédé, on arrive à une écriture dans laquelle n'apparait plus de produit XY. C'est la forme demandée par l'énoncé, et l'unicité est claire (je vous la laisse).

(2) Soit le morphisme $f' : k[x, y, z, t] \to B$ qui envoie x, z, t sur eux-mêmes et y sur ZT/X. Le polynôme $xy - zt$ est envoyé sur 0 donc f' se factorise en un morphisme $f : A \to B$. Montrons que f est injectif : si $f(a) = 0$ avec $a = a_0 + xa_1(x) + ya_2(y)$ comme dans (1), alors $a_0 + xa_1(X) + \frac{ZT}{X}a_2(\frac{ZT}{X}) = 0$. Regardons cela comme une égalité dans $R[X, 1/X]$ qui possède une base formée des puissances positives ou négatives de X. On voit que a_0 est constant, $Xa_1(X)$ ne possède que des monômes de degré (en X) strictement positif et $\frac{ZT}{X}a_2(\frac{ZT}{X})$ ne possède que des monômes de degré (en X) strictement négatif. Donc $a_0 = a_1 = a_2 = 0$ puis $a = 0$.

(3) On suppose que l'on a une écriture $z = ab$ dans A, avec $a = a_0 + xa_1(x) + ya_2(y)$ et $b = b_0 + xb_1(x) + yb_2(y)$. On utilise le morphisme injectif de la question (2), que l'on voit comme une injection, pour plonger cette égalité dans $B = k(x)[z, t]$, qui est un anneau de polynômes en deux variables sur un corps. On sait que z est un irréductible de B, donc a est inversible dans B i.e. $a \in k(x)$, et $b = a^{-1}z$ (ou l'inverse). Ceci implique que ni $a_0 + xa_1(x) + \frac{zt}{x}a_2(\frac{zt}{x})$ ni $b_0 + xb_1(x) + \frac{zt}{x}b_2(\frac{zt}{x})$ ne possèdent de monôme contenant t, donc :

$$a_0 \in k\ ,\ a_1 \in k[x]\ ,\ a_2 = 0 \qquad \text{et} \qquad b_0 \in k.z\ ,\ b_1 \in k[x].z\ ,\ b_2 = 0\ .$$

On voit ainsi que a est en fait un polynôme en x et b est produit de z par un polynôme en x. Pour avoir $z = ab$ on doit avoir $a \in k^*$ et $b = a^{-1}z$. Ceci montre que z est irréductible dans A. Le raisonnement pour t est symétrique. Pour montrer que x et y sont irréductibles, on fait pareil en utilisant des écritures $a_0 + za_1(z) + ta_2(t)$ avec les a_i à coefficients dans $k[x, y]$.

(4) Montrons par exemple que x n'est multiple ni de y ni de z, les autres cas sont semblables. Le fait que x n'est pas multiple de y est équivalent au fait que la classe de x est non nulle dans

$A/(y)$. Or on a $A/(y) \simeq k[x,y,z,t]/(xy-zt,y) \simeq k[x,z,t]/(zt)$ et il est clair que la classe de x est non nulle. Le fait que x n'est pas multiple de z est équivalent au fait que la classe de x est non nulle dans $A/(z)$, or $A/(z) \simeq k[x,y,z,t]/(xy-zt,z) \simeq k[x,y,t]/(xy)$ et il est clair que la classe de x est non nulle.

(5) L'élément xy possède deux écritures distinctes comme produit d'irréductibles : $xy = zt$.

(6) On commence par une petite observation : deux irréductibles distincts (c'est-à-dire, non associés) p et q ont 1 pour pgcd, car sinon ce pgcd est associé à p et à q, ce qui n'est pas possible. D'après l'exercice 1, si xz et xy ont un pgcd alors z et y en ont un et on a $\text{pgcd}(xz,xy) = x\text{pgcd}(z,y) = x$. Par ailleurs, $xy = zt$, de sorte que par le même raisonnement $\text{pgcd}(xz,xy) = \text{pgcd}(xz,zt) = z\text{pgcd}(x,t) = z$. Comme z et t ne sont pas associés, c'est une contradiction, donc xz et xy n'ont pas de pgcd.

(7) Les éléments x et z sont des irréductibles distincts donc ils ont un pgcd qui est $d = 1$. S'ils ont un ppcm m, d'après le résultat de l'exercice 3 on a la relation $xz = md = m$. Or $xy = zt$ est manifestement un multiple de x et de z, il doit donc être multiple de $m = xz$. Or xy multiple de xz implique y multiple de z, ce qui n'est pas le cas d'après la question (4). Donc x et z n'ont pas de ppcm. □