6 Anneaux euclidiens, principaux, factoriels

On cherche à dégager et étudier des classes d'anneaux intègres qui ont des propriétés arithmétiques similaires à celles de $\mathbf{Z}$ et $\mathbf{K}[X]$ (où $\mathbf{K}$ est un corps).

Parmi les motivations que l'on peut dégager :

- c'est joli et intéressant !
- cela peut permettre de résoudre des problèmes d'arithmétique sur $\mathbf{Z}$ (*cf.* la section consacrée à la motivation historique ci-dessous, ainsi que la section 6.4) ;
- (à plus long terme) dans le cadre de la géométrie algébrique, ces classes correspondent à des objets ayant de très bonnes propriétés géométriques ;
- cela peut *ne pas* permettre de résoudre des problèmes d'arithmétique sur $\mathbf{Z}$ (*cf.* encore une fois la section consacrée à la motivation historique ci-dessous, ainsi que la section 6.4...) ; cela apporte un éclairage instructif et conceptuel sur le fait que l'arithmétique est difficile, et peut entraîner le développement d'outils nouveaux et utiles (la notion abstraite d'idéal d'un anneau est née comme cela)

6.1 Motivation historique

Cette partie peut être réservée à une seconde lecture.

Lorsque l'on souhaite démontrer des résultats portant sur l'arithmétique de $\mathbf{Z}$, il peut s'avérer extrêmement utile de travailler sur un anneau plus gros ; ceci est illustré notamment dans la section 6.4 ci-dessous.

Une autre illustration frappante de ce procédé est la tentative de démonstration du « dernier théorème de Fermat » proposée en 1847 par le mathématicien Gabriel Lamé. Rappelons qu'il s'agit de démontrer l'énoncé suivant : pour tout entier $n \geqslant 3$, l'équation

$$x^n + y^n = z^n$$

n'a pas de solutions $(x, y, z) \in \mathbf{Z}^3$ non triviales (une solution (x, y, z) est dite triviale si $x\,y\,z = 0$, c'est-à-dire l'une des trois inconnues est nulle). L'approche proposée par Lamé était erronée [12], mais l'erreur commise était assez subtile, tout à fait « digne » du grand mathématicien qu'était Lamé et au final très intéressante, puisqu'elle est concomitante à la naissance de concepts fondamentaux en théorie des anneaux.

Avant d'expliquer les grandes lignes de l'idée de Lamé, rappelons l'énoncé suivant :

Proposition. *Soit $n \geqslant 2$ un entier, b et c des entiers relatifs premiers entre eux et $a = b\,c$. On suppose que $|a|$ est une puissance n-ème (c'est-à-dire s'écrit α^n où α est un entier relatif). Alors $|b|$ et $|c|$ sont aussi des puissances n-ème.*

La proposition se généralise à un produit quelconque de facteurs supposés premiers entre eux 2 à 2. Cette proposition ainsi que sa généralisation se démontrent à partir du théorème de

12. En fait l'énoncé ci-dessus n'a finalement été démontré dans toute sa généralité qu'en 1994 par Andrew Wiles.

décomposition en facteurs premiers. L'un des aspects les plus cruciaux de la démonstration est que l'on utilise l'*unicité* de la décomposition. Cette proposition se généralise à tout anneau intègre admettant une théorème de décomposition en irréductibles aux propriétés similaires à celui qui existe sur $\mathbf{Z}$; en particulier, et c'est absolument fondamental, on doit avoir en un certain sens unicité d'une telle décomposition. De tels anneaux sont appelés *anneaux factoriels* et seront définis plus précisément ci-dessous.

De fait, on a la généralisation de la proposition ci-dessus.

Proposition. *Soit A un anneau factoriel, soit $n \geqslant 2$ un entier, b et c des éléments de A premiers entre eux et $a = bc$. On suppose que a est associé à une puissance n-ème (c'est-à-dire à un élément qui s'écrit α^n où $\alpha \in A$). Alors b et c sont aussi associés à des puissances n-ème.*

Là encore, on peut généraliser à un produit fini de facteurs supposés premiers entre eux deux à deux.

L'idée de Lamé pour démontrer qu'il n'y a pas de solutions entières non triviales à l'équation $x^p + y^p = z^p$ pour p premier impair [13] est d'écrire l'équation sous la forme

$$\prod_{i=0}^{p-1} (x + \zeta_p^i\, y) = z^p \tag{6.1}$$

où ζ_p est une racine primitive p-ème de l'unité.

Ceci permet de voir l'équation (6.1) comme une égalité dans l'anneau noté $\mathbf{Z}[\zeta_p]$, défini comme le sous-anneau de $\mathbf{C}$ image de $\mathbf{Z}[X]$ par l'unique morphisme $\mathbf{Z}[X] \to \mathbf{C}$ qui envoie X sur ζ_p. Ainsi $\mathbf{Z}[\zeta_p] = \{P(\zeta_p), \quad P \in \mathbf{Z}[X]\}$.

Par des manipulations relativement standards, on montre que s'il existe un triplet $(x, y, z) \in \mathbf{Z}^3$ vérifiant (6.1), alors il en existe un tel que les éléments de $\mathbf{Z}[\zeta]$

$$x + \zeta_p\, y,\ x + \zeta_p^2\, y, \ldots, x + \zeta_p^{p-1}\, y \tag{6.2}$$

sont premiers entre eux deux à deux. Comme leur produit est d'après (6.1) une puissance p-ème, chacun de ces éléments est associés à une puissance p-ème. De ce dernier fait on arrive à déduire une contradiction.

L'idée de Lamé est très séduisante. Sa faiblesse fondamentale réside cependant dans l'étape consistant à montrer que les éléments (6.2) sont des puissances p-ème. En fait, on applique à ce stade la (généralisation de la) proposition 6.1. Le (*gros !*) problème est que l'anneau $\mathbf{Z}[\zeta_p]$ n'est en général pas factoriel. À l'époque où Lamé propose sa démonstration, l'existence d'anneaux non factoriels n'était vraiment pas une évidence, et il semblait naturel

13. Rappelons que sachant que le dernier théorème de Fermat est vrai pour $n = 4$, pour démontrer le théorème en toute généralité, il suffit de considérer des exposants premiers impairs

de penser que les propriétés de $\mathbf{Z}$ se généralisaient aisément [14] aux anneaux $\mathbf{Z}[\zeta_p]$. La stratégie de Lamé s'applique quand même dans certains cas.

Insistons lourdement sur le fait que le problème des anneaux $\mathbf{Z}[\zeta_p]$ en général n'est pas le défaut d'*existence* d'une décomposition en produit d'irréductibles. Cette propriété d'existence est en fait vraie pour *tous* les anneaux $\mathbf{Z}[\zeta_p]$. Ce qui fait défaut, ce qui est vraiment exigeant, est la propriété d'*unicité* de la décomposition.

Il est à noter également que le défaut de factorialité d'anneaux tel que les anneaux $\mathbf{Z}[\zeta_p]$ est justement ce qui a poussé Kummer et Dedekind à dégager la notion d'*idéal*, fondement de l'approche algébrique de la théorie des nombres et de l'algèbre moderne en général.

6.2 Euclide, Gauss, Bézout, factorisation unique

Il est très fortement recommandé de revoir si nécessaire les notions d'élément irréductible et d'éléments premiers entre eux dans un anneau intègre avant de lire ce qui suit (partie *Éléments irréductibles d'un anneau intègre* du chapitre 2).

Définition 1. Soit A un anneau intègre. On dit que A vérifie :

- *la propriété irréductible=premier* si : pour tout $a \in A$ tel que $a \neq 0$, alors l'idéal aA est premier si et seulement si a est irréductible ;
- *le lemme d'Euclide* si : pour tous $a, b, c \in A$ tels que a est irréductible et divise bc alors a divise b ou a divise c ;
- *le théorème de Bézout* si : pour tous $a, b \in A$, a et b sont premiers entre eux si et seulement si $aA + bA = A$;
- *le lemme de Gauss* si : pour tous $a, b, c \in A$ tels que a divise bc et a et b sont premiers entre eux alors a divise c ;
- *le théorème de factorisation unique en produit d'irréductibles* si : pour tout $a \in A \setminus (\{0\} \cup A^\times)$ alors il existe un entier strictement positif r et r éléments irréductibles $p_1, \ldots, p_r$ de A tels que $a = \prod_{i=1}^{r} p_i$; par ailleurs l'entier r et les éléments $p_1, \ldots, p_r$ vérifiant cette propriété sont uniques au sens suivant : supposons qu'il existe un entier strictement positif s et s éléments irréductibles $q_1, \ldots, q_s$ de A tels que $a = \prod_{i=1}^{s} q_i$; alors $s = r$ et, quitte à renuméroter les q_i et les p_i, pour tout $1 \leqslant i \leqslant r$, p_i et q_i sont associés

Dans la dernière propriété, l'unicité peut s'exprimer de la manière informelle suivante : « la factorisation est unique à l'ordre des facteurs et à l'association près. »

Exemples. On sait que l'anneau $\mathbf{Z}$ et, pour $\mathbf{K}$ un corps quelconque, l'anneau $\mathbf{K}[X]$ vérifient toutes les propriétés de la définition 1. On verra (ceci avait été admis lors de certains exercices de TD) qu'elles valent aussi par exemple pour l'anneau $\mathbf{Z}[i]$.

14. Bien sûr, en toute rigueur, Lamé aurait dû penser à le vérifier ; que celui qui n'est jamais tombé dans le piège d'une généralisation hâtive lui jette la première pierre... En fait, Kummer avait peu de temps auparavant justement démontré que cette généralisation n'était pas valide, mais Lamé n'était pas au courant de ce travail ; à l'époque, la circulation des nouvelles découvertes scientifiques n'était évidemment pas aussi aisée qu'actuellement !

On a vu dans l'exercice 2.5 que $\mathbf{Z}[i\sqrt{3}]$ ne vérifiait *pas* la propriété irréductible=premier. D'après la proposition 3 ci-dessous, $\mathbf{Z}[i\sqrt{3}]$ ne vérifie donc ni Bézout, ni Gauss, ni Euclide.

Par ailleurs, sans préjuger de l'existence générale d'une décomposition en produit d'irréductibles dans $\mathbf{Z}[i\sqrt{3}]$, on peut exhiber des exemples de décomposition « non uniques » dans cet anneau. On considère par exemple l'égalité :

$$4 = 2^2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$$

Dans l'exercice 2.5, on montrait que 2 était un élément irréductible de $\mathbf{Z}[i\sqrt{3}]$. Les mêmes arguments montrent que $(1 + i\sqrt{3})$ et $(1 - i\sqrt{3})$ sont des éléments irréductibles de $\mathbf{Z}[i\sqrt{3}]$. Si la décomposition de 4 en produits d'irréductibles était unique au sens de la définition 1, 2 serait nécessairement associé à $1 + i\sqrt{3}$. Or, toujours dans l'exercice 2.5, on montre que les éléments inversibles de $\mathbf{Z}[i\sqrt{3}]$ sont 1 et -1. Ainsi les seuls éléments de $\mathbf{Z}[i\sqrt{3}]$ associés à 2 sont 1 et -1. Donc dans l'anneau $\mathbf{Z}[i\sqrt{3}]$, l'élément 4 possède une décomposition en produit d'irréductibles, mais elle n'est pas unique au sens de la définition 1.

L'exemple de $\mathbf{Z}[i\sqrt{3}]$ montre que les propriétés de la définition 1 ne valent pas pour un anneau intègre quelconque. Cependant on a le résultat suivant.

Proposition 2. *Soit A un anneau intègre. Alors A vérifie :*

- la propriété « premier entraîne irréductible » *: soit $a \in A$ non nul ; si aA est un idéal premier, a est irréductible ;*
- le lemme d'Euclide faible : *soit $a, b, c \in A$; si aA est un idéal premier non nul et a divise bc alors a divise b ou a divise c ;*
- le théorème de Bézout faible : *soit $a, b \in A$; si $aA + bA = A$ alors a et b sont premiers entre eux.*
- le lemme de Gauss faible : *soit $a, b, c \in A$; si a divise bc et $aA + bA = A$ alors a divise c.*

Les différentes propriétés de la définition 1 ont des liens logiques entre elles, comme le montre la proposition suivante.

Proposition 3. *Soit A un anneau intègre. Alors on a les propriétés suivantes.*

1. *L'anneau A vérifie la propriété « irréductible=premier » si et seulement si A vérifie le lemme d'Euclide.*
2. *Si A vérifie le lemme de Gauss, A vérifie le lemme d'Euclide.*
3. *Si A vérifie le théorème de Bézout, alors A vérifie le lemme de Gauss.*

6.3 Anneaux factoriels, principaux, euclidiens

Nous définissons ici les trois grandes classes d'anneaux qui vont nous intéresser. Nous donnons quelques exemples et résultats importants, sans démonstration pour l'instant.

Définition 4. Soit A un anneau intègre. L'anneau A est dit *factoriel* s'il vérifie le théorème de factorisation unique en produit d'irréductibles (*cf.* définition 1).

Insistons encore une fois sur l'importance fondamentale de la propriété d'*unicité* de la factorisation : une simple propriété d'existence rendrait infiniment moins de services. D'ailleurs, la dénomination anglophone pour *anneau factoriel* est *unique factorization domain* (souvent abrégée en UFD) et met donc plus l'accent que la dénomination francophone sur cet aspect fondamental ; en outre l'emploi du terme *domain*, signifiant dans ce contexte *anneau intègre*, rappelle la condition d'intégrité dans la définition. La terminologie *unique factorization domain* est à rapprocher de la terminologie *factorization domain* évoquée dans la deuxième remarque qui suit la proposition 2.

Les anneaux principaux définis ci-dessous forment, comme on le verra, une classe importante d'anneaux factoriels.

Définition 5. Soit A un anneau intègre. L'anneau A est dit *principal* si tout idéal de A est engendré par un élément. En d'autres termes, pour tout idéal $\mathcal{I}$ de A, il existe $a \in A$ tel que $\mathcal{I} = aA$.

Les anneaux sur lesquels existe une division euclidienne forment, comme on le verra, une classe importante d'anneaux principaux.

Définition 6. Soit A un anneau intègre. L'anneau A est dit *euclidien* s'il existe une application

$$\nu \colon A \setminus \{0\} \to \mathbf{N}$$

vérifiant telle que pour tout $(a, b) \in A \times (A \setminus \{0\})$, il existe $(q, r) \in A^2$ tel que

$$a = bq + r \text{ et soit } r = 0, \text{ soit } \nu(r) < \nu(b).$$

Avant de donner des exemples et contre-exemples illustrant les notions définies précédemment, nous énonçons quelques résultats importants qui les concernent.

Théorème 7. *1. Il existe des anneaux intègres non factoriels.*

2. Tout anneau principal est factoriel

3. Il existe des anneaux factoriels non principaux.

4. Tout anneau euclidien est principal.

5. Il existe des anneaux principaux non euclidiens.

Théorème 8. *Soit A un anneau factoriel. Alors $A[X]$ est un anneau factoriel.*

Théorème 9. *Soit A un anneau factoriel. Alors A vérifie le lemme de Gauss (donc le lemme d'Euclide et la propriété « irréductible=premier »).*

Théorème 10. *Soit A un anneau principal. Alors A vérifie le théorème de Bézout (donc la propriété « irréductible=premier », le lemme d'Euclide et le lemme de Gauss). Ces propriétés sont donc en particulier vérifiée si A est un anneau euclidien.*

Par contre les anneaux factoriels ne vérifient pas le théorème de Bézout en général. Plus précisément :

Théorème 11. *Soit A un anneau factoriel. On suppose que A vérifie le théorème de Bézout. Alors A est principal.*

Tous les résultats énoncés précédemment seront démontrés ci-après, sauf l'existence d'anneaux principaux non euclidiens, un peu délicate [15].

Commençons par expliciter un certain nombre de (contre)-exemples.

Exemple. Soit $\mathbf{K}$ un corps. Les anneaux $\mathbf{Z}$ et $\mathbf{K}[X]$ sont euclidiens (donc principaux et factoriels), avec pour stathmes respectifs $\nu\colon n \mapsto |n|$ et $\nu\colon P \mapsto \deg(P)$. Dans les deux cas la division euclidiennt jouit en outre d'une propriété d'unicité ; mais cette propriété d'unicité n'est pas exigée dans la définition d'un anneau euclidien, et n'est pas toujours vérifiée, comme le montrera l'exemple de $\mathbf{Z}[i]$ ci-dessous.

Exemple. Soit $\mathbf{K}$ un corps. En vertu du théorème 8, on en déduit que pour tout entier strictement positif n, les anneaux $\mathbf{Z}[X_1, \ldots, X_n]$ et $\mathbf{K}[X_1, \ldots, X_n]$ sont factoriels. On verra ci-dessous que l'anneau $\mathbf{Z}[X_1, \ldots, X_n]$ n'est pas principal, et que si $n \geqslant 2$ l'anneau $\mathbf{K}[X_1, \ldots, X_n]$ n'est pas non plus principal.

15. Contentons nous de signaler que l'anneau $\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est l'un des exemples classiques d'anneau principal non euclidien.

Exemple. L'anneau des entiers de Gauss $\mathbf{Z}[i]$ est euclidien (donc principal et factoriel), de stathme $\nu\colon z \mapsto z\bar{z}$; *cf.* la proposition 12 ci-dessous.

Exemple. Soit $\mathbf{K}$ un corps. Rappelons que pour un élément $P = \sum_{n=0}^{+\infty} a_n X^n$ de l'anneau de séries formelles $\mathbf{K}[[X]]$, on définit la valuation $\nu(P)$ de P par

$$\nu(P) = \mathrm{Inf}\{n \in \mathbf{N}, \quad a_n \neq 0\}.$$

Alors $P \mapsto \nu(P)$ est un stathme euclidien sur $\mathbf{K}[[X]]$ (*cf.* l'exercice 5.1). En particulier l'anneau $\mathbf{K}[[X]]$ est euclidien, donc principal et factoriel. Noter que le fait que $\mathbf{K}[[X]]$ est un anneau principal découle de la question 13 de l'exercice 1.5. Et le théorème de factorisation unique en produit d'irréductibles pour $\mathbf{K}[[X]]$ peut se vérifier directement (*cf.* encore une fois l'exercice 5.1)

Exemple. Soit p un nombre premier. Alors la valuation p-adique ν_p (*cf.* la question 3 de l'exercice 1.7) est un stathme euclidien sur l'anneau $\mathbf{Z}_{(p)}$. En particulier l'anneau $\mathbf{Z}_{(p)}$ est euclidien, donc principal et factoriel. Noter que le fait que $\mathbf{Z}_{(p)}$ est un anneau principal découle de la question 3(d) de l'exercice 1.7. Et le théorème de factorisation unique en produit d'irréductibles pour $\mathbf{Z}_{(p)}$ peut se vérifier directement (*cf.* l'exercice 2.6).

Exemple. L'anneau $A = \mathbf{Z}[i\sqrt{3}]$, isomorphe au quotient $\mathbf{Z}[X]/\langle X^2 + 3\rangle$, est intègre mais n'est pas factoriel (déjà vu)

Exemple. Si $\mathbf{K}$ est un corps, l'anneau $A = \mathbf{K}[X,Y]/\langle X^2 - Y^3\rangle$ est intègre mais n'est pas factoriel. Intuitivement, ceci vient du fait que l'on a « forcé » dans le quotient la factorisation non unique $X^2 = Y^3$. Plus précisément, l'exercice 2 du deuxième contrôle continu de 2018 montre que A est intègre et que les images x et y de X et Y dans A sont irréductibles. L'égalité $x^2 = y^3$ montre alors que A ne peut pas être factoriel : en effet, il découle de la définition que dans un anneau factoriel, le nombre de facteurs irréductibles (« comptés avec multiplicité ») intervenant dans une décomposition est toujours le même.

Cet exemple et le précédent montrent qu'un quotient intègre d'un anneau factoriel n'est pas nécessairement factoriel.

Exemple. Si A est un anneau intègre, on montre que l'anneau $A[X]$ est principal si et seulement si A est un corps (*cf.* exercice 5.13). En vertu du théorème 8, les anneaux $\mathbf{Z}[X]$ et (si $\mathbf{K}$ est un corps) $\mathbf{K}[X,Y]$ sont donc des anneaux factoriels qui ne sont pas principaux. De fait, on peut vérifier que $\langle 2, X\rangle$ n'est pas un idéal principal de $\mathbf{Z}[X]$ (cette dernière question a été posée au deuxième contrôle continu de 2018) et que $\langle X, Y\rangle$ n'est pas un idéal principal de $\mathbf{K}[X,Y]$.

Proposition 12. *Sur l'anneau $\mathbf{Z}[i]$ des entiers de Gauss, on considère l'application « norme » :*

$$\begin{array}{ccc} \mathbf{Z}[i] & \longrightarrow & \mathbf{N} \\ z & \longmapsto & N(z) = z\bar{z} = |z|^2 \end{array}.$$

Alors N induit sur $\mathbf{Z}[i] \setminus \{0\}$ un stathme euclidien. En particulier l'anneau $\mathbf{Z}[i]$ est euclidien (donc principal et factoriel).

Exemple. Comme on l'a déjà signalé, la démonstration ci-dessus fournit une procédure effective pour calculer les divisions euclidiennes dans $\mathbf{Z}[i]$

À titre d'exemple, calculons une (en fait plusieurs) division euclidienne de $5+10i$ par $-1+7i$. Commençons par calculer dans $\mathbf{C}$ le quotient du dividende par le diviseur sous forme algébrique :

$$\frac{5+10i}{-1+7i} = \frac{(5+10i)(-1-7i)}{|-1+7i|^2} = \frac{65-45i}{50} = \frac{13}{10} - \frac{9}{10}i.$$

Il s'agit à présent de déterminer un élement de $\mathbf{Z}[i]$ qui est à distance < 1 de $\frac{13}{10} - \frac{9}{10}i$. La « maille » de $\mathbf{Z}[i]$ qui contient ce dernier élément est le carré de sommets 1, 2, $2-i$ et $1-i$. Tous sauf 2 sont à distance < 1 de $\frac{13}{10} - \frac{9}{10}i$.

Ainsi on peut prendre par exemple $q = 1$ et $r = (5+10i) - (-1+7i) = 6+3i$. On obtient que $5+10i = 1.(-1+7i) + (6+3i)$ est une division euclidienne de $5+10i$ par $-1+7i$.

On peut aussi prendre $q = 1-i$ et $r = (5+10i) - (1-i)(-1+7i) = -1+2i$. On obtient que $5+10i = (1-i).(-1+7i) + (-1+2i)$ est une autre division euclidienne de $5+10i$ par $-1+7i$.

On peut enfin prendre $q = 2-i$ et $r = (5+10i) - (2-i)(-1+7i) = -5i$. On obtient que $5+10i = (2-i).(-1+7i) + (-5i)$ est également une division euclidienne de $5+10i$ par $-1+7i$.

6.4 Applications : caractérisation des nombres premiers qui sont somme de deux carrés

(*cf.* les exercices 1.7.1, 2.20 et 3.14) Nous donnons ici une application du fait que l'anneau des entiers de Gauss $\mathbf{Z}[i]$ vérifie la propriété « irréductible=premier » à un problème arithmétique qui concerne initialement les entiers « classiques », à savoir : quels sont les nombres premiers qui s'écrivent comme somme de deux carrés ?

Rappelons que i désigne un nombre complexe dont le carré vaut -1 et que $\mathbf{Z}[i] := \{a+ib, \quad (a,b) \in \mathbf{Z}^2\}$ est sous-anneau de $\mathbf{C}$ contenant $\mathbf{Z}$, qui peut aussi être défini comme étant l'image de l'unique morphisme de $\mathbf{Z}$-algèbres de $\mathbf{Z}[X]$ vers $\mathbf{C}$ qui envoie X sur i. Le noyau de ce dernier morphisme est l'idéal engendré par X^2+1, de sorte que $\mathbf{Z}[i]$ est isomorphe à l'anneau quotient $\mathbf{Z}[X]/\langle X^2+1\rangle$.

L'application norme

$$N : \begin{array}{ccc} \mathbf{C} & \longrightarrow & \mathbf{R}^+ \\ z & \longmapsto & |a|^2 = z\bar{z} \end{array}$$

vérifie $\forall z_1, z_2 \in \mathbf{C}$, $N(z_1 z_2) = N(z_1)N(z_2)$ et induit par restriction et corestriction une application $N\colon \mathbf{Z}[i] \to \mathbf{N}$. L'ensemble $\mathbf{Z}[i]^\times$ des éléments inversibles de $\mathbf{Z}[i]$ est égal à $\{z \in \mathbf{Z}[i], \quad N(z) = 1\}$ (on peut décrire explicitement ce dernier ensemble, mais nous ne nous en servirons pas dans ce qui suit).

Théorème 13. *Soit p un nombre premier. Les propriétés suivantes sont équivalentes :*

1. *p n'est pas un élément irréductible de $\mathbf{Z}[i]$;*
2. *l'idéal $p\mathbf{Z}[i]$ n'est pas un idéal premier de $\mathbf{Z}[i]$;*
3. *-1 est un carré modulo p ; en d'autres termes $[-1]_p$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$;*
4. *p est une somme de carrés d'entiers ; en d'autres termes il existe $(a, b) \in \mathbf{Z}^2$ tels que $a^2 + b^2 = p$.*

Notons que l'équivalence entre (3) et (4) exprime une propriété relevant uniquement de l'arithmétique sur $\mathbf{Z}$.

6.5 Valuations dans un anneau factoriel

Si p est un nombre premier, on a rencontré en TD (*cf.* notamment l'exercice 1.7.3) la notion de valuation p-adique. Rappelons que la valuation p adique d'un entier non nul est la plus grande puissance de p qui divise cet entier. Entre autres propriétés extrêmement utiles, cette notion vérifie par exemple que pour toute paire d'entiers, la valuation p-adique de leur produit est égale à la somme des valuations p-adiques de chacun d'entre eux. On a également vu une notion similaire de valuation sur les anneaux de séries formelles, avec des propriétés strictement analogues si l'anneau des coefficients est un anneau intègre.

On peut se demander dans quelle mesure cette notion existe pour d'autres anneaux intègres. Considérons par exemple le cas de $A = \mathbf{Z}[i\sqrt{3}]$ (*cf.* l'exercice 2.5 pour la définition et les propriétés utiles). Comme 2 est un élément irréductible de A, on peut imaginer définir ainsi la notion de valuation 2-adique sur A : $v_2(0) = +\infty$ et pour $a \in A \setminus \{0\}$, $v_2(a)$ est le plus grand entier positif n tel que 2^n divise a. Notons que pour tout $a \in A \setminus \{0\}$ et $n \in \mathbf{N}$ tels que 2^n divise a, alors $4^n = N(2^n)$ divise $N(a)$ dans $\mathbf{Z}$. Ainsi l'ensemble des $n \in \mathbf{N}$ tel que 2^n divise a est majoré, ce qui montre que $v_2(a)$ est bien définie. Cependant, 2 ne divise pas $1 + i\sqrt{3}$, en d'autres termes $v_2(1 + i\sqrt{3}) = 0$. Supposons en effet qu'il existe $b \in \mathbf{Z}[i\sqrt{3}]$ tel que $2b = 1 + i\sqrt{3}$. En prenant la norme, on en déduit aussitôt $N(b) = 1$, soit $b \in \{1, -1\}$, ce qui est contradictoire car $1 + i\sqrt{3} \notin \mathbf{Z}$. De même on voit que $v_2(1 + i\sqrt{3}) = 0$. Ainsi

$$v_2(1 + i\sqrt{3}) + v_2(1 - i\sqrt{3}) = 0$$

tandis que

$$v_2((1 + i\sqrt{3})(1 - i\sqrt{3})) = v_2(2^2) = 2$$

On perd donc la propriété « valuation du produit=somme des valuations », ce qui limite considérablement l'intérêt de la valuation 2-adique sur $\mathbf{Z}[i\sqrt{3}]$.

Rappelons par ailleurs que $\mathbf{Z}[i\sqrt{3}]$ n'est pas factoriel. Dans ce qui suit, on va voir que la notion de valuation p-adique sur $\mathbf{Z}$ s'étend avec les propriétés voulues aux anneaux factoriels. *Si ce qui suit vous paraît un peu technique, il est conseillé de garder en permanence en tête l'exemple « familier » de* $A = \mathbf{Z}$.

Soit A un anneau intègre. La relation « est associé à » est notée $\sim$ et est une relation d'équivalence sur A. Notons que pour tous éléments a, b de l'ensemble $A/\sim$, d'après la remarque qui suit la définition 63 du chapitre 2, on peut donner un sens à la condition « a divise b »

La relation $\sim$ induit une relation d'équivalence sur l'ensemble des éléments irréductibles de A. Soit $\mathscr{I}(A)$ l'ensemble quotient de l'ensemble des éléments irréductibles de A par cette relation d'équivalence. Dans la pratique, il est utile de travailler avec un système de représentants $\mathrm{Irr}(A) \subset A$ de $\mathscr{I}(A)$, que l'on pourra parfois (notamment pour alléger les notations) identifier à $\mathscr{I}(A)$.

Exemples. Si $A = \mathbf{Z}$, on peut prendre pour $\mathrm{Irr}(A)$ l'ensemble des nombres premiers (qui n'est autre que l'ensemble des éléments irréductibles positifs de $\mathbf{Z}$).

Si $\mathbf{K}$ est un corps et $A = \mathbf{K}[X]$, on peut prendre pour $\mathrm{Irr}(A)$ l'ensemble des polynômes irréductibles unitaire.

Si $\mathbf{K}$ est un corps et $A = \mathbf{K}[[X]]$, on peut prendre pour $\mathrm{Irr}(A)$ le singleton $\{X\}$.

Si p est un nombre premier et $A = \mathbf{Z}_{(p)}$, on peut prendre pour $\mathrm{Irr}(A)$ le singleton $\{p\}$.

Si x est un entier non nul et $A = \mathbf{Z}[\frac{1}{x}]$, on peut prendre pour $\mathrm{Irr}(A)$ l'ensemble des nombres premiers qui ne divisent pas x.

Théorème 14. *Soit A un anneau factoriel. Soit a un élément non nul de A. Alors il existe une unique famille presque nulle $(v_\pi(a)) \in \mathbf{N}^{(\mathscr{I}(A))}$ d'entiers indexée par $\mathscr{I}(A)$ telle que pour tout système $\mathrm{Irr}(A)$ de représentants d'irréductibles de A, on a*

$$a \sim \prod_{\pi \in \mathrm{Irr}(A)} \pi^{v_\pi(a)}.$$

Définition 15. Soit A un anneau factoriel et $\pi \in \mathscr{I}(A)$. En posant $v_\pi(0) = +\infty$, le théorème précédent permet de définir une fonction

$$\begin{array}{ccc} A & \longrightarrow & \mathbf{N} \cup \{+\infty\} \\ a & \longmapsto & v_\pi(a) \end{array}$$

appelée « valuation π-adique » et qui vérifie

$$\forall a \in A, \quad v_\pi(a) = +\infty \Leftrightarrow a = 0.$$

Théorème 16. *Soit A un anneau factoriel.*

1. *Soit $a, b \in A$. Alors a et b sont associés si seulement si pour tout $\pi \in \mathscr{I}(A)$, on a $v_\pi(a) = v_\pi(b)$.*
2. *Soit $a \in A$. Alors a est inversible si et seulement si pour tout $\pi \in \mathscr{I}(A)$, on a $v_\pi(a) = 0$.*
3. *Soit $a, b \in A$. Alors pour tout $\pi \in \mathscr{I}(A)$, on a*
$$v_\pi(ab) = v_\pi(a) + v_\pi(b).$$
4. *Soit $a, b \in A$. Alors a divise b si et seulement si pour tout $\pi \in \mathscr{I}(A)$, on a $v_\pi(a) \leqslant v_\pi(b)$.*
5. *Soit $a \in A$ un éléments non nul et $\pi \in \mathscr{I}(A)$. Alors*
$$v_\pi(a) = \mathrm{Max}\{n \in \mathbf{N}, \quad \pi^n \text{ divise } a\}.$$

6.6 Plus grand commun diviseur, plus petit commun multiple ; cas des anneaux factoriels, principaux, euclidiens ; relations de Bézout, algorithme d'Euclide étendu

Les notions de pgcd et de ppcm et leurs propriétés sont bien connues dans le cas des anneaux $\mathbf{Z}$ ou $\mathbf{K}[X]$ (où $\mathbf{K}$ est un corps). On généralise ici la notion à un anneau intègre quelconque. La différence fondamentale est qu'en général les pgcd et ppcm n'existent pas toujours (*cf.* l'exercice 5.10.7). On verra que c'est cependant le cas dans les anneaux factoriels, et qu'on peut calculer facilement les pgcd et les ppcm d'éléments dont on connaît une décomposition en irréductibles (chose que vous avez sans doute déjà vue pour $\mathbf{Z}$ et $\mathbf{K}[X]$). Par contre l'analogue du théorème de Bézout n'est vraie que sur les anneaux principaux. Pour mémoire : $\mathbf{Z}[X]$ et $\mathbf{K}[X, Y]$ sont des exemples standards d'anneaux factoriels non principaux.

6.6.1 pgcd, ppcm

Définition 17. Soit A un anneau intègre et $a, b \in A$. Un pgcd de la paire $\{a, b\}$ est un élément $\delta \in A$ vérifiant les propriétés suivantes :

1. δ divise a et b ;
2. soit $d \in A$ qui divise a et b ; alors d divise δ.

Un ppcm de la paire $\{a, b\}$ est un élément $\mu \in A$ vérifiant les propriétés suivantes :

1. a et b divisent μ ;

2. soit $m \in A$ qui est divisible par a et b ; alors m est divisible par μ.

Exemple. Si a et b sont des éléments de A premiers entre eux, tout élément de $A^\times$ est un pgcd de a et b.

Si a et b sont des éléments associés de A, tout élément associé à a et b est un pgcd de a et b.

Pour tout élément a de A, tout élément associé à a est un pgcd de a et 0. En particulier, 0 est un pgcd de 0 et 0. Par ailleurs si a et b sont des éléments de A qui admettent 0 pour pgcd, alors 0 divise a et b, et donc $a = b = 0$.

Encore une fois, nous verrons en TD qu'en général, les pgcd et ppcm n'existent pas toujours. Par contre un pgcd ou un ppcm, s'ils existent, sont uniquement déterminés à association près. La démonstration de la proposition qui suit fait aussi l'objet d'un exercice de TD.

Proposition 18. *Soit A un anneau intègre et $a, b \in A$. On suppose que a et b admettent un pgcd δ (respectivement un ppcm μ).*

1. *Soit $c \in A$. Alors c est un pgcd (respectivement un ppcm) de a et b si et seulement si c est associé à δ (respectivement à μ).*
2. *Soit $\alpha \in A$. Alors $\alpha\delta$ (respectivement $\alpha\mu$) est un pgcd (respectivement un ppcm) de $\alpha\, a$ et $\alpha\, b$.*
3. *Soit $\alpha \in A \setminus \{0\}$ un diviseur commun de a et b. Alors $\frac{\delta}{\alpha}$ (respectivement $\frac{\mu}{\alpha}$) est un pgcd (respectivement un ppcm) de $\frac{a}{\alpha}$ et $\frac{b}{\alpha}$.*
   En particulier, si $\delta \neq 0$, (ou ce qui revient au même si $(a, b) \neq (0, 0)$), $\frac{a}{\delta}$ et $\frac{b}{\delta}$ sont premiers entre eux.

Dans un anneau factoriel, les pgcd et ppcm existent toujours.

Théorème 19. *Soit A un anneau factoriel et $a, b \in A$.*

1. *Soit $c \in A$. Alors :*
   (a) *c est un pgcd de a et b si et seulement si pour tout $\pi \in \mathscr{I}(A)$ on a*
   $$v_\pi(c) = \mathrm{Min}(v_\pi(a), v_\pi(b)) \ ;$$
   (b) *c est un ppcm de a et b si et seulement si pour tout $\pi \in \mathscr{I}(A)$ on a*
   $$v_\pi(c) = \mathrm{Max}(v_\pi(a), v_\pi(b)).$$

En particulier a et b admettent un pgcd et un ppcm.

2. *Supposons en outre A principal. Alors :*
   (a) *c est un pgcd de a et b si et seulement si c engendre $aA + bA$;*
   (b) *c est un ppcm de a et b si et seulement si c engendre $aA \cap bA$.*

6.6.2 Relations de Bézout

Définition 20. Soit A un anneau intègre et $a, b \in A$. Une *relation de Bézout* pour a et b est un couple $(u, v) \in A^2$ tel que $au + bv$ est un pgcd de a et b.

Proposition 21. *Soit A un anneau intègre et $a, b \in A$. Alors il existe une relation de Bézout pour a et b si et seulement si l'idéal $aA + bA$ est principal.*

Ainsi, si A est principal, toute paire d'éléments de A admet une relation de Bézout. Dans la pratique, la détermination effective d'une telle relation (qui intervient par exemple lorsque l'on souhaite expliciter l'isomorphisme réciproque du théorème chinois) n'est pas un problème facile. Cependant, dans le cas particulier d'un anneau euclidien, et pour peu que la division euclidienne soit effective, on dispose d'une procédure efficace pour calculer des relations de Bézout.

6.6.3 Algorithme d'Euclide étendu dans un anneau euclidien

On utilisera le lemme élémentaire suivant.

Lemme 22. *Soit A un anneau intègre et α, β des éléments de A. On suppose qu'il existe $q, r \in A$ vérifiant*

$$\alpha = q\beta + r.$$

Alors la paire $\{\alpha, \beta\}$ admet un pgcd si et seulement si la paire $\{\beta, r\}$ admet un pgcd. En outre, dans ce cas, les paires $\{\alpha, \beta\}$ et $\{\beta, r\}$ ont les mêmes pgcd.

Soit A un anneau euclidien et ν un stathme euclidien sur A. Soit $a, b \in A$. On décrit l'algorithme d'Euclide étendu, qui permet de calculer une relation de Bézout pour a et b (donc en particulier un pgcd de a et b). Il s'agit d'une extension immédiate de l'algorithme

d'Euclide étendu sur $\mathbf{Z}$ et $\mathbf{K}[X]$ ($\mathbf{K}$ un corps) que vous avez très probablement déjà rencontrés dans vos études.

Notons que si $b = 0$, a est un pgcd de a et b et $a = 1 \cdot a + 0 \cdot b$ est une relation de Bézout pour a et b. Dans tout ce qui suit, on supposera que b est non nul.

Commençons par décrire l'algorithme d'Euclide « non étendu », qui permet de calculer un pgcd de a et b par divisions euclidiennes successives.

On initialise l'algorithme d'Euclide en posant $r_{-1} = a$ et $r_0 = b$. Ensuite, pour n entier positif, et tant que r_n est non nul, on écrit une division euclidienne de r_{n-1} par r_n :

$$r_{n-1} = q_n r_n + r_{n+1}.$$

En particulier, $r_{n+1} = 0$ ou $\nu(r_{n+1}) < \nu(r_n)$. On définit ainsi une suite $(r_n)_{n\geqslant -1}$ d'éléments de A qui est nécessairement une suite finie, car la suite $(\nu(r_n))_{n\geqslant 0}$, définie tant que r_n n'est pas nul, est une suite strictement décroissant d'entiers positifs. D'après le lemme 22, une récurrence immédiate montre que pour tout n tel que r_{n+1} est défini les paires $\{a, b\}$ et $\{r_n, r_{n+1}\}$ ont les mêmes pgcd. Ainsi si N est le plus grand entier positif n tel que $r_n \neq 0$, les paires $\{a, b\}$ et $\{r_N, r_{N+1}\} = \{r_N, 0\}$ ont les mêmes pgcd. En particulier r_N (le « dernier reste non nul ») est un pgcd de a et b.

Il est possible de calculer une relation de Bézout pour a et b à partir de l'algorithme d'Euclide en « remontant » les divisions euclidiennes. Vous avez sans doute déjà rencontré ce genre de manipulations pour $\mathbf{Z}$ ou $\mathbf{K}[X]$. Si cette méthode est assez efficace lorsque le nombre d'étapes dans l'algorithme d'Euclide est petit, elle possède en particulier l'inconvénient pratique de nécessiter de « garder en mémoire » toutes les étapes de l'algorithme. L'algorithme d'Euclide étendu, que l'on présente maintenant, n'a pas ce défaut.

Plutôt que de donner directement les formules de cet algorithme, expliquons l'idée qui permet de les retrouver facilement. Elle consiste à construire récursivement, pour n allant de -1 à N, une combinaison linéaire de a et b (ici et dans ce qui suit, « combinaison linéaire » s'entend à coefficients dans A) égale à r_n. Ainsi pour $n = N$, on obtiendra la relation de Bezout cherchée. Pour $n = -1$ et $n = 0$, de telles combinaisons sont données « gratuitement » par

$$a.1 + b.0 = r_{-1} = a \quad \text{et} \quad a.0 + b.1 = r_0 = b$$

(mais en fait toutes autres combinaisons linéaire de a et b égales à a d'une part et b d'autre part conviendraient pour initialiser l'algorithme) Supposons à présent que pour un $n \in \{0, \ldots, N-1\}$ on connaisse $(u_{n-1}, v_{n-1}) \in A^2$ et $(u_n, v_n) \in A^2$ tels que

$$a.u_{n-1} + b.v_{n-1} = r_{n-1} \quad \text{et} \quad a.u_n + b.v_n = r_n$$

Toute combinaison linéaire de deux combinaisons linéaires de a et b est encore une combinaison linéaire de a et b. L'idée pour déterminer une combinaison linéaire de a et b égale à r_{n+1} est de partir d'une combinaison linéaire de r_{n-1} et r_n égale à r_{n+1} En effet, si $(\alpha_n, \beta_n) \in A^2$

vérifie $\alpha_n r_{n-1} + \beta_n r_n = r_{n+1}$, en ajoutant α_n fois la première des combinaisons ci-dessus à β_n fois la seconde, on obtiendra une combinaison linéaire de a et b égale à r_{n+1}. Or une combinaison linéaire de r_{n-1} et r_n égale à r_{n+1} intervient naturellement dans l'algorithme d'Euclide : la division euclidienne $r_{n-1} = q_n r_n + r_{n+1}$ se réécrit $1.r_{n-1} + (-q_n).r_n = r_{n+2}$.

On obtient ainsi la description suivante de l'algorithme d'Euclide étendu. On initialise l'algorithme en posant $r_{-1} := a$, $u_{-1} := 1$, $v_{-1} := 0$, $r_0 := b$, $u_0 := 0$, $v_0 := 1$. Ensuite, pour n entier positif, et tant que r_n est non nul, on écrit une division euclidienne de r_{n-1} par r_n :

$$r_{n-1} = q_n r_n + r_{n+1}$$

ce qui définit r_{n+1}. En outre on pose

$$u_{n+1} := u_{n-1} - q_n\, u_n, \quad v_{n+1} := v_{n-1} - q_n\, v_n.$$

Désignant toujours par N le plus grand entier positif n que $r_n \neq 0$, on a alors, pour tout entier n vérifiant $-1 \leqslant n \leqslant N$

$$r_n = u_n r_{-1} + v_n r_0$$

en particulier

$$\mathrm{pgcd}(a, b) = r_N = u_N r_{-1} + v_N r_0.$$

6.6.4 pgcd, ppcm d'une famille finie d'éléments

Les notions de pgcd et de ppcm d'une paire d'éléments s'étendent au cas d'une famille finie d'éléments, avec des énoncés strictement analogues. Les démonstrations sont essentiellement identiques. Encore une fois, si ce qui vous suit vous paraît un peu technique, gardez constamment à l'esprit l'exemple familier de $\mathbf{Z}$ à titre d'illustration.

Définition 23. Soit A un anneau intègre, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de A indexée par I.

Les éléments de la famille $\{a_i\}_{i\in I}$ sont dits premiers entre eux si les seuls diviseurs communs à tous les a_i sont les inversibles de A.

Un pgcd de la famille $\{a_i\}_{i\in I}$ est un élément $\delta \in A$ vérifiant les propriétés suivantes :

1. pour tout $i \in I$, δ divise a_i ;
2. soit $d \in A$ tel que pour tout $i \in I$, d divise a_i ; alors d divise δ.

Un ppcm de la famille $\{a_i\}_{i\in I}$ est un élément $\mu \in A$ vérifiant les propriétés suivantes :

1. pour tout $i \in I$, a_i divise μ ;
2. soit $m \in A$ tel que pour tout $i \in I$, a_i divise m ; alors μ divise m.

Proposition 24. *Soit A un anneau intègre, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de A indexée par I. On suppose que la famille $\{a_i\}_{i\in I}$ admet un pgcd δ (respectivement un ppcm μ).*

1. *Soit $c \in A$. Alors c est un pgcd (respectivement un ppcm) de la famille $\{a_i\}_{i\in I}$ si et seulement si c est associé à δ (respectivement à μ).*
2. *Soit $\alpha \in A$. Alors $\alpha\delta$ (respectivement $\alpha\mu$) est un pgcd (respectivement un ppcm) de la famille $\{\alpha a_i\}_{i\in I}$.*
3. *Soit $\alpha \in A \setminus \{0\}$ un diviseur commun à tous les a_i. Alors $\frac{\delta}{\alpha}$ (respectivement $\frac{\mu}{\alpha}$) est un pgcd (respectivement un ppcm) de la famille $\{\frac{a_i}{\alpha}\}_{i\in I}$.*
   En particulier, si $\delta \neq 0$, (ou ce qui revient au même si les a_i ne sont pas tous nuls) les éléments de la famille $\{\frac{a_i}{\delta}\}_{i\in I}$ sont premiers entre eux.
4. *δ est un pgcd de la famille $\{a_i\}_{i\in I} \cup \{0\}$.*

Théorème 25. *Soit A un anneau factoriel, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de A indexée par I.*

1. *Soit $c \in A$. Alors :*
   (a) *c est un pgcd de la famille $\{a_i\}_{i\in I}$ si et seulement si pour tout $\pi \in \mathscr{I}(A)$ on a*
   $$v_\pi(c) = \mathrm{Min}_{i\in I}(v_\pi(a_i)) \ ;$$
   (b) *c est un ppcm de la famille $\{a_i\}_{i\in I}$ seulement si pour tout $\pi \in \mathscr{I}(A)$ on a*
   $$v_\pi(c) = \mathrm{Max}_{i\in I}(v_\pi(a_i)).$$
   En particulier la famille $\{a_i\}_{i\in I}$ admet un pgcd et un ppcm.
2. *Supposons en outre A principal. Alors :*
   (a) *c est un pgcd de la famille $\{a_i\}_{i\in I}$ si et seulement si c engendre l'idéal $\sum_{i\in I} a_i A$;*
   (b) *c est un ppcm de la famille $\{a_i\}_{i\in I}$ si et seulement si c engendre $\cap_{i\in I} a_i A$.*

Définition 26. Soit A un anneau intègre, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de A indexée par I. Une *relation de Bézout* pour la famille $\{a_i\}_{i\in I}$ est une famille $\{u_i\}_{i\in I}$ d'éléments de A indexée par I telle que $\sum_{i\in I} a_i u_i$ est un pgcd de la famille $\{a_i\}_{i\in I}$.

Proposition 27. *Soit A un anneau intègre, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de A indexée par I. Alors il existe une relation de Bézout pour la famille $\{a_i\}_{i\in I}$ si et seulement si l'idéal $\sum_{i\in I} a_i A$ est un idéal principal.*

6.7 Valuations, pgcd et ppcm dans le corps des fractions d'un anneau factoriel

Les notions de valuations, pgcd et ppcm sur un anneau factoriel peuvent être étendues à peu de frais au corps des fractions de cet anneau. L'utilité de cette extension apparaîtra dans la section suivante. Comme toujours, si ce qui suit vous paraît un peu technique, gardez constamment en tête l'exemple de $A = \mathbf{Z}$, pour lequel $\mathrm{Frac}(A) = \mathbf{Q}$; vous pouvez par exemple traiter les exercices ci-dessous sous cette hypothèse.

L'exemple suivant est sans doute déjà assez illustratif : soit $a = \frac{9}{4} = 2^{-2}.3^2.7^0$ et $b = \frac{3}{14} = 2^{-1}.3.7^{-1}$; alors $\nu_2(a) = -2$, $\nu_2(b) = -1$, $\nu_3(a) = 2$, $\nu_3(b) = 1$, $\nu_7(a) = 0$, $\nu_7(b) = -1$. Un $\mathbf{Z}$-pgcd de a et b est $2^{-2}.3.7^{-1} = \frac{3}{28}$ et un $\mathbf{Z}$-ppcm de a et b est $2^{-1}.3^2.7^0 = \frac{9}{2}$.

Lemme 28. *Soit A un anneau factoriel et $x \in \mathrm{Frac}(A)$. Soit $\pi \in \mathscr{I}(A)$. Soit $(a, b) \in A \times A \setminus \{0\}$ tel que $x = \frac{a}{b}$. Alors l'élément $v_\pi(a) - v_\pi(b) \in \mathbf{N} \cup \{+\infty\}$ ne dépend que de x et pas du choix d'un tel couple (a, b), et coïncide avec $v_\pi(x)$ si $x \in A$.*

Définition 29. Soit A un anneau factoriel et $x \in \mathrm{Frac}(A)$. Soit $\pi \in \mathscr{I}(A)$. Soit $(a, b) \in A \times A \setminus \{0\}$ tel que $x = \frac{a}{b}$. Alors

$$v_\pi(x) := v_\pi(a) - v_\pi(b)$$

est appelé la valuation π-adique de x

Notons que si A est un anneau intègre la relation d'équivalence « est associé à » s'étend aux élément de $\mathrm{Frac}(A)$: deux éléments x, y de $\mathrm{Frac}(A)$ seront dits A-associés s'il existe un élément $\alpha \in A^\times$ vérifiant $x = \alpha y$. On note $\sim_A$ la relation de A-association. La dénomination « A-associés » (et non simplement « associés ») est là pour éviter les confusions possibles venant du fait qu'il n'y a en général pas unicité de l'anneau intègre A dont le corps des fractions est $\mathrm{Frac}(A)$. Par exemple $\frac{1}{2}$ et $-\frac{1}{2}$ sont $\mathbf{Z}$-associés, tandis que $\frac{1}{2}$ et 2 sont $\mathbf{Q}$-associées mais pas $\mathbf{Z}$-associés.

Théorème 30. *Soit A un anneau factoriel.*

1. *Soit x un élément non nul de* $\mathrm{Frac}(A)$*. Alors pour tout élément $\pi \in \mathscr{I}(A)$ sauf un nombre fini, $v_\pi(x)$ est nul. Par ailleurs, pour tout système* $\mathrm{Irr}(A)$ *de représentants d'irréductibles de A, on a*
$$x \sim_A \prod_{\pi \in \mathrm{Irr}(A)} \pi^{v_\pi(x)}.$$
Cette dernière formule s'étend au cas $x = 0$ avec la convention $\pi^{+\infty} = 0$
2. *Soit $x, y \in \mathrm{Frac}(A)$. Alors x et y sont A-associés si et seulement si pour tout $\pi \in \mathscr{I}(A)$, on a*
$$v_\pi(x) = v_\pi(y).$$
3. *Soit $x \in \mathrm{Frac}(A)$. Alors $x \in A$ si et seulement si pour tout $\pi \in \mathscr{I}(A)$, on a $v_\pi(x) \geqslant 0$.*
4. *Soit $x, y \in \mathrm{Frac}(A)$. Alors pour tout $\pi \in \mathscr{I}(A)$, on a*
$$v_\pi(xy) = v_\pi(x) + v_\pi(y).$$

Définition 31. Soit A un anneau factoriel, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments non nuls de $\mathrm{Frac}(A)$ indexée par I.

Pour $\pi \in \mathscr{I}(A)$, soit
$$N_\pi := \mathrm{Min}_{i\in I}(v_\pi(a_i))$$
et
$$M_\pi := \mathrm{Max}_{i\in I}(v_\pi(a_i)).$$

On appelle A-pgcd de la famille $\{a_i\}_{i\in I}$ tout élément de $\mathrm{Frac}(A)$ qui est A-associé à $\prod_{\pi\in\mathscr{I}(A)} \pi^{N_\pi}$ (avec la convention $\pi^{+\infty} = 0$).

On appelle A-ppcm de la famille $\{a_i\}_{i\in I}$ tout élément de $\mathrm{Frac}(A)$ qui est A-associé à $\prod_{\pi\in\mathscr{I}(A)} \pi^{M_\pi}$ (avec la même convention que ci-dessus).

Proposition 32. *Soit A un anneau factoriel, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de* $\mathrm{Frac}(A)$ *indexée par I.*

1. *Supposons que pour tout $i \in I$, on a $a_i \in A$. Alors tout A-pgcd (resp. tout A-ppcm) de $\{a_i\}_{i\in I}$ est un pgcd (resp. un A-ppcm) de de $\{a_i\}_{i\in I}$*
2. *Les conditions suivantes sont équivalentes :*
   (a) pour tout $i \in I$, $a_i \in A$;

(b) tout A-pgcd de la famille $\{a_i\}_{i\in I}$ est dans A ;

(c) un A-pgcd de la famille $\{a_i\}_{i\in I}$ est dans A.

On a des énoncés analogues à certains énoncés de la proposition 24.

Proposition 33. *Soit A un anneau factoriel, I un ensemble fini non vide et $\{a_i\}_{i\in I}$ une famille d'éléments de* $\mathrm{Frac}(A)$ *indexée par I. Soit δ un A-pgcd (resp. un A-ppcm) de la famille $\{a_i\}_{i\in I}$.*

1. *Soit $\alpha \in \mathrm{Frac}(A)$. Alors $\alpha\delta$ (respectivement $\alpha\mu$) est un A-pgcd (respectivement un A-ppcm) de la famille $\{\alpha a_i\}_{i\in I}$.*
2. *Soit $\alpha \in \mathrm{Frac}(A)\setminus\{0\}$. Alors $\frac{\delta}{\alpha}$ (respectivement $\frac{\mu}{\alpha}$) est un A-pgcd (respectivement un A-ppcm) de la famille $\{\frac{a_i}{\alpha}\}_{i\in I}$.*
3. *δ est un A-pgcd de la famille $\{a_i\}_{i\in I}\cup\{0\}$.*

6.8 Factorialité des anneaux de polynômes, critères d'irréductibilité

Dans cette section, on démontre en particulier le théorème 8, à savoir le résultat suivant : si A est un anneau factoriel, $A[X]$ est factoriel. On donne également, pour un anneau factoriel, des critères d'irréductibilté dans $A[X]$ et dans $\mathrm{Frac}(A)[X]$. Il est important dans ce qui suit de bien avoir assimilé les notions de A-associations et de A-pgcd définies dans la section précédente. *Il peut être utile (voire conseillé), en première lecture, de supposer dans tout ce qui suit que $A = \mathbf{Z}$.*

Définition 34. Soit A un anneau factoriel et $P \in \mathrm{Frac}(A)[X]$ un polynôme. On appelle contenu du polynôme P, et on note $c(P)$, tout A-pgcd des coefficients de P.

On dit que le polynôme P est primitif si $c(P) \sim_A 1$.

Proposition 35. *Soit A un anneau factoriel et $P \in A[X]$.*

1. *Si P est le polynôme nul, $c(P) = 0$, et ceci caractérise le polynôme nul.*
2. *Soit $P \in A[X]$ un polynôme unitaire. Alors P est primitif.*
   Plus généralement, si $P \in \mathrm{Frac}(A)[X]$ est unitaire, alors $\frac{1}{c(P)} \in A$.
3. *Soit $P \in \mathrm{Frac}(A)[X]$. On a $P \in A[X]$ si et seulement si $c(P) \in A$. En particulier tout polynôme primitif de* $\mathrm{Frac}(A)[X]$ *est un élément de $A[X]$.*

4. *Pour tout* $a \in \mathrm{Frac}(A)$*, on a* $c(aP) \sim_A ac(P)$*.*
5. *On suppose* $P \neq 0$*. Alors* $c(P) \neq 0$ *et* $\frac{P}{c(P)}$ *est un polynôme primitif.*

Proposition 36. *Soit* A *un anneau factoriel et* $P, Q \in \mathrm{Frac}(A)[X]$*. Alors* $c(PQ) \sim_A c(P)c(Q)$*.*

Lemme 37. *Soit* A *un anneau factoriel,* $P \in A[X]$ *un polynôme primitif,* $Q, R \in \mathrm{Frac}(A)[X]$ *tels que* $P = QR$*. Alors il existe des éléments primitifs* $\tilde{Q}$*,* $\tilde{R}$ *de* $A[X]$*, associés respectivement à* Q *et* R *dans* $\mathrm{Frac}(A)[X]$*, et tels que* $P = \tilde{Q}\tilde{R}$*.*

Théorème 38. *Soit* A *un anneau factoriel. L'ensemble des éléments irréductibles de* $A[X]$ *est la réunion disjointes des deux ensembles suivants :*

1. *l'ensemble des polynômes constants qui sont des éléments irréductibles de* A
2. *l'ensemble des polynômes qui sont primitifs et irréductibles dans* $\mathrm{Frac}(A)[X]$

Exemple. Tout polynôme *unitaire* de degré 1 est un élément irréductible de $A[X]$. Mais si a est un élément non nul et non inversible de A, le polynôme $aX + a$ est un polynôme de degré 1 qui n'est pas irréductible dans $A[X]$.

Corollaire 39. *Si* A *est un anneau factoriel et* n *est un entier strictement positif, l'anneau* $A[X_1, \ldots, X_n]$ *est factoriel.*

En particulier, si $\mathbf{K}$ *est un corps, l'anneau* $\mathbf{K}[X_1, \ldots, X_n]$ *est factoriel.*

Nous terminons ce chapitre par quelques critères d'irréductibilité dans les anneaux de polynômes.

Basiquement, l'idée est la suivant : soit A et B des anneaux intègres et $\varphi\colon A \to B$ un morphisme d'anneaux. Si $f \in A[X]$ a un coefficient dominant non tué par φ et est un produit de deux polynômes non constants, $\varphi(f)$ sera un produit de deux polynômes non constants

dans $B[X]$. Par contraposée, des propriétés d'« irréductibilité » de $\varphi(f)$ conduiront à des propriétés d'« irréductibilité » de f. L'exemple le plus basique est le résultat suivant (vu en TD) : soit $\mathbf{K} \to \mathbf{L}$ une extension de corps et $P \in \mathbf{K}[X]$; si P est irréductible dans $\mathbf{L}[X]$, il l'est aussi dans $\mathbf{K}[X]$. De manière générale, des critères efficaces sont obtenues en prenant pour φ un certain morphisme quotient, mais il faut faire attention au sens d'irréductible dans l'anneau $A[X]$ lorsque A n'est plus un corps (d'où les guillemets ci-dessus). Ceci motive notamment l'hypothèse de factorialité dans les énoncés ci-dessous.

Théorème 40. *Soit A un anneau factoriel, π un élément irréductible de A, B l'anneau intègre $A/\pi A$ et $\varphi\colon A \to B$ le morphisme quotient. On note encore φ l'unique morphisme d'anneau $A[X] \to B[X]$ qui envoie X sur X et induit φ en restriction à A (morphisme de « réduction modulo π » des coefficients d'un polynôme de $A[X]$)*

Soit $P \in A[X]$. On suppose que $\deg(\varphi(P)) = \deg(P)$ *et que $\varphi(P)$ est irréductible dans* $\mathrm{Frac}(A/\pi)[X]$. *Alors P est irréductible dans* $\mathrm{Frac}(A)[X]$.

Exemple. On peut appliquer ce critère à $X^4 + X^3 + 2X + 3 \in \mathbf{Z}[X]$ et $\pi = 2$. En effet on peut montrer que $X^4 + X^3 + [1]_2$ est irréductible dans $\mathbf{F}_2[X]$: il n'a pas de racine dans $\mathbf{F}_2$ et il n'est pas divisible par l'unique polynôme irréductible de degré 2 de $\mathbf{F}_2[X]$, à savoir $X^2 + X + [1]_2$.

On peut aussi appliquer ce critère à $X^2 + 1 + XYR(Y) + YS(Y) \in \mathbf{R}[X, Y]$ et $\pi = Y$.

Le critère d'Eisenstein est également un critère d'irréductibilité basé sur la réduction modulo un irréductible π, mais de manière un peu plus fine, puisque dans le cadre d'application de ce critère le polynôme réduit modulo π sera réductible, ce qui permettra quand même au vu des hypothèses faites de conclure à l'irréductibilité du polynôme initial via une analyse plus poussée.

Théorème 41. Critère d'Eisenstein

Soit A un anneau factoriel, π un élément irréductible de A, B l'anneau intègre $A/\pi A$ et $\varphi\colon A \to B$ le morphisme quotient. On note encore φ l'unique morphisme d'anneau $A[X] \to B[X]$ qui envoie X sur X et induit φ en restriction à A (morphisme de « réduction modulo π » des coefficients d'un polynôme de $A[X]$)

Soit $n \geqslant 1$ un entier et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ un polynôme de degré n.

On suppose que pour tout $0 \leqslant i \leqslant n-1$, π divise a_i, que π ne divise pas a_n et que π^2 ne divise pas a_0.

Alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Exemple. Pour tout nombre premier p et tout entier strictement positif n, le polynôme $X^n - p$ est irréductible dans $\mathbf{Q}[X]$ (et dans $\mathbf{Z}[X]$) ; pour le voir, on applique Eisenstein avec $\pi = p$. Il existe donc des polynômes irréductibles de tout degré dans $\mathbf{Q}[X]$.

Exemple. Soit $\mathbf{K}$ un corps, n un entier strictement positif et $P(Y) \in \mathbf{K}[Y]$ tel que $P(0) \neq 0$. Alors le polynôme $X^n - YP(Y)$ est irréductible dans $\mathbf{K}[X, Y]$. Pour le voir on applique Eisenstein avec $A = \mathbf{K}[Y]$ et $\pi = Y$.

6.9 Démonstration des résultats de la section 6.3

On présente les démonstration manquantes des résultats de la section 6.3 du chapitre 6, à l'exception de l'existence d'anneaux principaux non euclidiens.

6.9.1 Tout anneau euclidien est principal

Commençons par démontrer que tout anneau euclidien est principal, c'est-à-dire le point 4 du théorème 7. En un sens, il n'y a strictement rien de nouveau par rapport aux démonstrations déjà connues du fait que $\mathbf{Z}$ et $\mathbf{K}[X]$ ($\mathbf{K}$ un corps) sont principaux, démonstrations basées de manière cruciale sur la division euclidienne.

Soit donc A un anneau euclidien, et ν un stathme euclidien sur A. Par définition d'un anneau euclidien, A est intègre.

Soit $\mathcal{I}$ un idéal de A. Il s'agit de montrer qu'il existe $a \in A$ tel que $\mathcal{I} = aA$. Si $\mathcal{I} = \{0\}$, $a = 0$ convient. On suppose à présent $\mathcal{I} \neq \{0\}$. On peut donc considérer le plus petit élément ν_0 de la partie non vide de $\mathbf{N}$ égale à $\nu(\mathcal{I} \setminus \{0\})$, et $a \in \mathcal{I} \setminus \{0\}$ un élément tel que $\nu(a) = \nu_0$. Montrons que $\mathcal{I} = aA$. Comme $a \in \mathcal{I}$, on a l'inclusion $aA \subset \mathcal{I}$. Soit à présent $b \in \mathcal{I}$. Soit $b = aq + r$ une division euclidienne de b par a (rappelons que a est non nul). En particulier on a $r = 0$ ou $\nu(r) < \nu(a) = \nu_0$. Mais par ailleurs on a $r = b - aq$ donc $r \in \mathcal{I}$. Si $r \neq 0$, on a donc $r \in \mathcal{I} \setminus \{0\}$ et $\nu(r) < \nu_0$ contredit la définition de ν_0. Donc $r = 0$ et $b = aq$, et finalement $b \in aA$. Donc $\mathcal{I} \subset aA$, d'où on déduit $\mathcal{I} = aA$

6.9.2 Tout anneau principal vérifie Bézout, Gauss et Euclide

Démontrons à présent le théorème 10.

Soit A un anneau principal. D'après la proposition 3, il suffit de montrer que A vérifie le théorème de Bézout. Soit $a, b \in A$ premiers entre eux. Il s'agit de montrer que $aA + bA = A$ (rappelons que la réciproque est vraie sur n'importe quel anneau intègre). Comme A est principal, il existe $d \in A$ tel que $aA + bA = dA$. En particulier $aA \subset dA$, donc d divise a. De même d divise b. Comme a et b sont premiers entre eux, d est inversible, donc $dA = A$ et $aA + bA = A$.

6.9.3 Tout anneau factoriel vérifie Gauss et Euclide

On démontre le théorème 9.

On va en fait démontrer un résultat en peu plus général.

Théorème 42. *Soit A un anneau intègre. On suppose que tout élément de A non nul et non inversible s'écrit comme un produit d'éléments irréductibles de A. Alors les propriétés suivantes sont équivalentes ,*

1. *A est factoriel ;*
2. *A vérifie le lemme de Gauss ;*
3. *A vérifie le lemme d'Euclide.*

6.9.4 Tout anneau principal est factoriel

On va utiliser le théorème 42 pour montrer que tout anneau principal est factoriel : on sait déjà que tout anneau principal vérifie Euclide ; il suffit donc de montrer que dans un anneau principal tout élément non nul et non inversible est un produit d'éléments irréductibles.

Soit donc A un anneau principal. Montrons tout d'abord que tout élément a de A non nul et non inversible est divisible par un élément irréductible de A. Comme a est non inversible, aA est un idéal propre de A, et est donc contenu dans un idéal maximal $\mathfrak{M}$ de A. Comme A est principal, il existe $\pi \in A$ tel que $\mathfrak{M} = \pi A$. Comme l'idéal $\mathfrak{M}$ est maximal et contient $a \neq 0$, il est premier et non nul. Donc π est irréductible. Comme aA est contenu dans πA, π divise a.

Lemme 43. *Soit $(\mathcal{I}_n)_{n\in\mathbf{N}}$ une suite croissante (pour l'inclusion) d'idéaux de A. Alors la suite est stationnaire, en d'autres termes il existe $n \in \mathbf{N}$ tel que pour tout $m \geqslant n$ on a $\mathcal{I}_m = \mathcal{I}_n$.*

Soit alors $a \in A$ un élément non nul et non inversible. Montrons que a est un produit d'éléments irréductibles. D'après le résultat précédent, il existe un élément irréductible π_1 tel que π_1 divise a. Soit $a_1 = \frac{a}{\pi_1}$. En particulier, a_1 est non nul. Si a_1 est inversible, a est irréductible et on a terminé. Sinon, il existe un élément irréductible π_2 de A qui divise a_1. Si $a_2 = \frac{a_1}{\pi_2}$ est inversible, on a terminé. Sinon, il existe un élément irréductible π_3 de A qui divise a_2... Il s'agit de voir que ce procédé se termine, en utilisant le lemme ci-dessus.

En fait on va associer à a deux suites $(\pi_n)_{n\geqslant 1}$ et $(a_n)_{n\geqslant 0}$ d'éléments de A telles que $a_0 = a$ et pour tout $n \in \mathbf{N} \setminus \{0\}$ on a : π_n est irréductible ou $\pi_n = 1$,

$$a = a_n \prod_{i=1}^{n} \pi_i, \text{et} \quad a_{n+1}\pi_{n+1} = a_n$$

On construit cette suite par récurrence en commençant comme indiqué ci-dessus pour (a_1, π_1). Supposons la suite $(a_i, \pi_i)_{i \leqslant n}$ construite. Si a_n est inversible, on pose $\pi_{n+1} = 1$ et $a_{n+1} = a_n$ Sinon, il existe un élément irréductible π_{n+1} de A qui divise a_n et on pose $a_{n+1} = \frac{a_n}{\pi_{n+1}}$

Pour tout $n \in \mathbf{N}$, posons $\mathcal{I}_n := a_n A$. Soit $n \in \mathbf{N}$. L'égalité $a_{n+1}\pi_{n+1} = a_n$ montre que $a_n \in a_{n+1}A$, d'où $a_n A \subset a_{n+1}A$. Ainsi la suite $(\mathcal{I}_n)$ est croissante. D'après le lemme ci-dessus, il existe $n_0 \in \mathbf{N}$ tel que $a_{n_0}A = a_{n_0+1}A$. Ainsi a_{n_0} et a_{n_0+1} sont associés. Comme $a_{n_0+1}\pi_{n_0+1} = a_{n_0}$ et un élément irréductible n'est pas inversible, on voit que π_{n_0+1} n'est pas irréductible. D'après la construction de la suite (a_n, π_n) ceci montre que a_{n_0} est inversible. Comme $a = a_{n_0} \prod_{i=1}^{n_0} \pi_i$, ceci conclut la démonstration.

6.9.5 Tout anneau factoriel qui vérifie Bezout est principal

Soit A un anneau factoriel vérifiant le théorème de Bezout. On va montrer que A est principal. Comme A est factoriel, A est intègre. Il reste à démontrer que tout idéal de A est principal, c'est à dire est engendré par un élément.

Commençons par montrer que tout idéal de A engendré par un nombre fini d'éléments est principal. Soit $a, b \in A$ et I l'idéal engendré par a et b. Si $a = b = 0$, $I = \{0\} = 0\,A$. Sinon a et b admettent un pgcd δ non nul. Montrons que $aA + bA = \delta A$. Comme δ divise a et b, on a $aA \subset \delta A$ et $bA \subset \delta A$, donc $aA + bA \subset \delta A$. Par ailleurs $\alpha := \frac{a}{\delta}$ et $\beta := \frac{b}{\delta}$ sont premiers entre eux. Comme A vérifie le théorème de Bezout, on a $\alpha A + \beta A = A$. Ainsi il existe $(u, v) \in A^2$ tels que $\alpha u + \beta v = 1$. En multipliant la relation précédente par δ, on obtient $\delta \in aA + bA$. Comme δA est l'idéal engendré par δ, on en déduit l'inclusion $\delta A \subset aA + bA$, d'où finalement l'égalité $aA + bA = \delta A$.

Ainsi tout idéal de A engendré par deux éléments est principal. Une récurrence facile montre alors que tout idéal de A engendré par un nombre fini d'éléments est principal.

Montrons ensuite que dans un anneau factoriel toute suite croissante (pour l'inclusion) d'idéaux principaux est stationnaire. Soit $(a_n) \in A^{\mathbf{N}}$ une suite d'éléments de A telle que la suite d'idéaux $(a_n A)_{n \in \mathbf{N}}$ est croissante pour l'inclusion. En d'autres termes, pour tout $n \in \mathbf{N}$, a_{n+1} divise a_n. Pour tout élément irréductible π de A, on obtient alors que la suite d'entiers positifs $(v_\pi(a_n))_{n \in \mathbf{N}}$ est décroissante, donc stationnaire. Par ailleurs, pour tout élément irréductible π de A qui ne divise pas a_0, $(v_\pi(a_n))_{n \in \mathbf{N}}$ est la suite nulle. On en déduit qu'il existe $N_0 \in \mathbf{N}$ tel que pour tout élément irréductible π de A la suite $(v_\pi(a_n))_{n \geqslant N_0}$ est constante (égale à disons ν_π). Soit $a = \prod_{\pi \in \mathscr{I}(A)} \pi^{\nu_\pi}$. Alors pour tout $n \geqslant N_0$, a_n et a, ayant les mêmes valuations adiques, sont associés. Ainsi pour tout $n \geqslant N_0$, on a $a_n A = aA$, ce qui conclut.

Montrons enfin que tout idéal I de A est principal. Soit I un idéal de A. On construit par récurrence une suite (I_n) d'idéaux de A contenus dans I de la façon suivante : soit $a_0 \in I$. On pose $I_0 = a_0 A$. Pour $n \in \mathbf{N}$, supposons l'idéal I_n construit. Si $I_n = I$, on pose $I_{n+1} = I$; sinon, il existe $a_{n+1} \in I \setminus I_n$; on pose alors $I_{n+1} = I_n + a_{n+1}A$; notons que dans ce dernier cas, I_{n+1} contient strictement I_n. Il est immédiat que (I_n) est croissante, et on

montre par une récurrence facile que pour tout $n \geqslant 0$, I_n est engendré par un nombre fini d'éléments, donc est principal d'après un résultat montré ci-dessus. Toujours d'après un résultat montré ci-dessus, la suite (I_n) est stationnaire, en particulier il existe $n_0 \in \mathbf{N}$ tel que $I_{n_0} = I_{n_0+1}$. D'après la construction de (I_n) on a alors $I = I_{n_0}$, donc I est principal.