Chapitre 7

Arithmétique des anneaux

Le but de ce chapitre est d'introduire l'*arithmétique des anneaux* généraux, en l'illustrant principalement sur les anneaux A de la forme $\mathbb{Z}[\sqrt{d}]$. Il s'agit d'étudier la relation de divisibilité, et de comprendre quelles propriétés arithmétiques de l'anneau $\mathbb{Z}$ des entiers, ou de l'anneau des polynômes $k[X]$ avec un corps, persistent en général. Par exemple, est-ce que tout élément de A s'écrit de manière unique comme produit d'éléments premiers/irréductibles ? (*théorème fondamental de l'arithmétique*). On dit que A est *factoriel* si cette propriété est vraie. Bien sûr, il nous faudra d'abord préciser ces notions (divisibilité, irréductibilité, relation d'association, etc...).

C'est Gauss qui le premier a rigoureusement démontré que l'anneau $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ (*entiers de Gauss*) est factoriel, et qui l'a appliqué à l'étude des sommes de deux carrés dans $\mathbb{Z}$ (méthode de l'*arithmétique transcendante*). Comme nous le verrons, cela permet non seulement de redémontrer que tout premier $\equiv 1 \bmod 4$ est somme de deux carrés, mais aussi de voir (de manière limpide !) qu'il l'est d'une unique manière. C'est aussi la propriété de factorialité qui rend de grands services dans l'étude des équations diophantiennes (comme l'équation de Fermat $x^n + y^n = z^n$). Nous détaillerons l'exemple plus simple mais historiquement important de l'équation $y^2 = x^3 - 2$.

Une notion clé est celle d'*idéal* d'un anneau. Elle généralise celle d'élément (Kummer parle d'élément "idéal"), ces derniers correspondants alors aux idéaux *principaux*. L'analogue de la divisibilité pour les idéaux est simplement la *contenance* $\supset$ ("contenir c'est diviser"). De ce point de vue, les idéaux se comportent mieux que les éléments ! Par exemple pgcd et ppcm existent toujours (sommes et intersections), et certaines questions de base se reformulent alors en terme de principalité de certains idéaux. Les anneaux les plus simples de ce point de vue sont ceux, dit *principaux*, dans lesquels tout idéal est principal. On démontre qu'ils sont factoriels. De plus, les anneaux *euclidiens*, dans lesquels une variante de la division euclidienne existe, sont automatiquement principaux. On a donc la hierarchie

$$\text{euclidien} \implies \text{principal} \implies \text{factoriel}.$$

Nous verrons que ces trois classes d'anneaux sont distinctes.

Une étude plus poussée des anneaux $\mathbb{Z}[\sqrt{d}]$, par exemple des substituts à la non factorialité, dépasse le cadre ce cours (*théorie algébrique des nombres*). Les concepts de ce chapitre s'appliquent aussi avec intérêt à d'autres types d'anneaux, par exemple à $\mathbb{C}[x_1, \ldots, x_n]$ et à ses quotients par un idéal I. Ils sont alors souvent un lien avec les propriétés géométriques de la sous-variété *algébrique* de $\mathbb{C}^n$ définie par l'annulation des éléments de I. Nous n'aborderons pas non plus ces aspects, qui appartiennent plus à un second cours d'algèbre (*géométrie algébrique*).

RÉFÉRENCES : On pourra consulter le chapitre 4 du livre de Stewart & Tall, le chapitre 1 du livre de Samuel, le chapitre du *Cours d'algèbre* de Perrin concernant l'arithmétique des anneaux, ou le cours de votre serviteur à l'École Polytechnique Théorie algébrique des nombres.

1. Les anneaux $\mathbb{Z}[\sqrt{d}]$

Un exemple historiquement important d'anneaux dont l'arithmétique est intéressante est celui des anneaux d'*entiers algébriques*. Nous nous contenterons ici de considérer le cas des entiers *quadratiques*. Fixons donc $d \in \mathbb{Z}$ *non carré*, ainsi qu'une racine carrée $\sqrt{d} \in \mathbb{C}$ de d. Son choix aura peu d'importance, mais pour fixer les idées on suppose $\sqrt{d} > 0$ pour $d > 0$ (cas dit *réel*), et $\sqrt{d}$ de partie imaginaire > 0 pour $d < 0$ (cas dit *imaginaire*). On considère les sous-groupes additifs de $\mathbb{C}$

$$\mathbb{Z}[\sqrt{d}] \subset \mathbb{Q}[\sqrt{d}] \subset \mathbb{C},$$

avec $\mathbb{Z}[\sqrt{d}] := \mathbb{Z} + \mathbb{Z}\sqrt{d}$ et $\mathbb{Q}[\sqrt{d}] := \mathbb{Q} + \mathbb{Q}\sqrt{d}$. Ces deux sous-groupes contiennent 1 et sont des sous-anneaux de $\mathbb{C}$ car on a la formule :

$$(x + y\sqrt{d})(x' + y'\sqrt{d}) \;=\; (xx' + dyy') \;+\; (xy' + x'y)\,\sqrt{d}. \tag{57}$$

REMARQUE 1.1. (i) L'anneau $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ s'appelle l'anneau des *entiers de Gauss*. Il sera utile pour étudier les sommes de deux carrés dans $\mathbb{Z}$ à cause de la factorisation $a^2 + b^2 = (a + bi)(a - bi)$ dans $\mathbb{Z}[i]$.

(ii) L'anneau $\mathbb{Z}[\sqrt{d}]$ sera par exemple utile pour étudier les solutions d'une équation diophantienne comme $y^2 = x^3 + d$ avec $x, y \in \mathbb{Z}$, à cause de la factorisation $(y - \sqrt{d})(y + \sqrt{d}) = x^3$.

(iii) Pour $d < 0$, on constate que $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ est un réseau de $\mathbb{C}$, alors que pour $d > 0$, c'est un sous-groupe dense de $\mathbb{R}$.

Noter que $\mathbb{Q}[\sqrt{d}]$ est même un sous $\mathbb{Q}$-espace vectoriel de $\mathbb{C}$. La famille $1, \sqrt{d}$ en est une base car d n'est pas un carré dans $\mathbb{Z}$, et donc dans $\mathbb{Q}$. C'est donc aussi une $\mathbb{Z}$-base du groupe additif $\mathbb{Z}[\sqrt{d}]$. Pour $x, y \in \mathbb{Q}$, et $z := x + y\sqrt{d}$, on pose

$$\begin{cases} \overline{z} = x - y\sqrt{d}, & \text{le } \textit{conjugué} \text{ de } z, \\ \mathrm{T}(z) = z + \overline{z} = 2x, & \text{la } \textit{trace} \text{ de } z, \\ \mathrm{N}(z) = z\overline{z} = x^2 - dy^2, & \text{la } \textit{norme de } z. \end{cases} \tag{58}$$

On a donc $z^2 - \mathrm{T}(z)z + \mathrm{N}(z) = 0 = (z - z)(z - \overline{z})$ (*identité de Cayley-Hamilton*).

LEMME 1.2. *(i)* $z \mapsto \overline{z}$ *est un automorphisme des anneaux* $\mathbb{Q}[\sqrt{d}]$ *et* $\mathbb{Z}[\sqrt{d}]$.
(ii) $\mathbb{Q}[\sqrt{d}]$ *est le corps des fractions de* $\mathbb{Z}[\sqrt{d}]$.
(iii) $\mathrm{N} : \mathbb{Q}[\sqrt{d}]^\times \to \mathbb{Q}^\times$ *est un morphisme de groupes et on a* $\mathrm{N}(\mathbb{Z}[\sqrt{d}]) \subset \mathbb{Z}$.

DÉMONSTRATION — L'application $z \mapsto \overline{z}$ est manifestement un endomorphisme $\mathbb{Q}$-linéaire de $\mathbb{Q}[\sqrt{d}]$ vérifiant $\overline{1} = 1$. De plus, pour $a, b \in \mathbb{Q}[\sqrt{d}]$ la Formule (57) montre $\overline{ab} = \overline{a}\,\overline{b}$, puis le (i). Pour $b \neq 0$, on a $\mathrm{N}(b) \in \mathbb{Q}^\times$ puis $a/b = ab/\mathrm{N}(b) \in \mathbb{Q}[\sqrt{d}]$, ce qui montre le (ii). Le (i) montre aussi $\mathrm{N}(ab) = ab\overline{ab} = ab\overline{a}\,\overline{b} = \mathrm{N}(a)\mathrm{N}(b)$, puis le (iii). □

REMARQUE 1.3. Pour $d < 0$, $\overline{z}$ n'est rien d'autre que le conjugué complexe de z, et $\mathrm{N}(z) = |z|^2$ est le carré de la norme $|.|$ usuelle sur $\mathbb{C}$. En particulier, on a $\mathrm{N}(z) \geqslant 0$ pour tout z.

Terminons ce paragraphe en examinant le groupe des inversibles de $\mathbb{Z}[\sqrt{d}]$.

LEMME 1.4. *On a* $\mathbb{Z}[\sqrt{d}]^\times = \{z \in \mathbb{Z}[\sqrt{d}] \mid \mathrm{N}(z) = \pm 1\}$.

DÉMONSTRATION — En effet, si $ab = 1$ dans $\mathbb{Z}[\sqrt{d}]$ on a $\mathrm{N}(a)\mathrm{N}(b) = \mathrm{N}(1) = 1$, puis $\mathrm{N}(a), \mathrm{N}(b) \in \mathbb{Z}^\times = \{\pm 1\}$. Réciproquement, si on a $\mathrm{N}(a) = \epsilon$ avec $a \in \mathbb{Z}[\sqrt{d}]$ et $\epsilon = \pm 1$, on a $a\overline{a} = \epsilon$ avec $\overline{a} \in \mathbb{Z}[\sqrt{d}]$, et donc $\epsilon\overline{a} = a^{-1} \in \mathbb{Z}[\sqrt{d}]$. □

Dans le cas $d < 0$, l'équation $x^2 - dy^2 = \pm 1$, avec $x, y \in \mathbb{Z}$, est triviale à résoudre.

COROLLAIRE 1.5. *On a* $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ *et* $\mathbb{Z}[\sqrt{d}]^\times = \{\pm 1\}$ *pour* $d < -1$.

La situation est assez différente pour $d > 0$. Dans ce cas, l'équation $x^2 - dy^2 = 1$ est appelée *équation de Pell-Fermat*, et a une très riche histoire. On vérifie facilement sur des exemples qu'elle a toujours des solutions (x, y) avec $y \neq 0$. Par exemple on a $3^2 - 2 \cdot 2^2 = 1$ pour $d = 2$. Nous renvoyons à l'Exercice 7.7 pour une démonstration de cette propriété en général (Lagrange). On en déduit le résultat suivant :

PROPOSITION 1.6. *Soit* $d > 0$ *non carré. Alors tout élément* > 1 *de* $\mathbb{Z}[\sqrt{d}]^\times$ *est de la forme* $x + y\sqrt{d}$ *avec* $x, y \in \mathbb{Z}_{\geqslant 1}$. *De plus, il existe un unique plus petit tel élément* η_d, *appelé unité fondamentale de* $\mathbb{Z}[\sqrt{d}]$, *et on a* $\mathbb{Z}[\sqrt{d}]^\times = \langle -1, \eta_d \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Par exemple, prenons $d = 2$. On a $1+\sqrt{2} > 1$ et $\mathrm{N}(1+\sqrt{2}) = -1$ donc $\eta_2 = 1+\sqrt{2}$. On en déduit par exemple $\eta_2^6 = (1 + \sqrt{2})^6 = 99 + 70\sqrt{2}$ et donc $99^2 - 2 \cdot 70^2 = 1$.

DÉMONSTRATION — Soit $u = x + y\sqrt{d}$ dans $\mathbb{Z}[\sqrt{d}]^\times \smallsetminus \{\pm 1\}$. Quitte à remplacer u par $-u$, on peut supposer $u > 0$, puis quitte à le remplacer par $1/u$ on peut supposer $u > 1$. Mais l'ensemble de 4 inversibles $\{u, u^{-1}, -u, -u^{-1}\} = \{\pm u, \pm\overline{u}\} = \{\pm x \pm y\sqrt{d}\}$ rencontre chacun des intervalles

$$]-\infty, -1[,\ ]-1, 0[,\ ]0, 1[\text{ et }]1, \infty[$$

en un point. Le plus grand des 4 est u, ce qui montre $x, y > 0$, et la première assertion. On en déduit que le sous-groupe des inversibles > 0 de $\mathbb{Z}[\sqrt{d}]$ est discret dans le groupe multiplicatif $\mathbb{R}_{>0}^\times \overset{\log}{\simeq} \mathbb{R}$. Comme il est non trivial par l'Exercice 7.7, la Proposition 7.3 Chap. 2 montre qu'il est monogène engendré par η_d. □

d	2	3	5	6	7	8	10	11	12
η_d	$1+\sqrt{2}$	$2+\sqrt{3}$	$2+\sqrt{5}$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{8}$	$3+\sqrt{10}$	$10+3\sqrt{11}$	$7+2\sqrt{12}$

TABLE 1. L'unité fondamentale de $\mathbb{Z}[\sqrt{d}]$ pour $0 < d \leqslant 12$.

2. Vocabulaire de la divisibilité

Dans tout ce paragraphe, A désigne un anneau *commutatif*. On supposera aussi que A est *intègre*, ce qui signifie qu'il est non nul, et que pour tout $a, b \in A$, $ab = 0$ entraîne $a = 0$ ou $b = 0$. Tout sous-anneau d'un corps est intègre.

DÉFINITION 2.1. *Si $a, b \in A$, on dit que « a divise b », ou que « b est multiple de a », et on écrit $a|b$, s'il existe $c \in A$ tel que $b = ac$.*

L'intégrité de A assure que le c ci-dessus est unique si $a \neq 0$. Pour tout $a, b, c \in A$, alors $a|a$, et si $a|b$ et $b|c$ alors $a|c$. Autrement dit, la relation de divisibilité est une relation de *préordre* sur A au sens de Bourbaki. Son étude est souvent appelée *arithmétique de A*. Par exemple, l'arithmétique d'un corps est inintéressante car deux éléments non nuls se divisent toujours l'un l'autre.

DÉFINITION 2.2. (Relation d'association) *On dit que $a, b \in A$ sont associés si on a $b|a$ et $a|b$. C'est une relation d'équivalence sur A que l'on notera $a \sim b$.*

Les diviseurs de 1 sont exactement les éléments inversibles de A. C'est pourquoi on les appelle aussi *unités* de A. Ils divisent tout élément de A.

LEMME 2.3. *Pour $a, b \in A$, on a $b|a$ et $a|b$ $\iff$ il existe $u \in A^\times$ avec $a = bu$.*

DÉMONSTRATION — Si on a $a = bu$ avec $u \in A^\times$, on a aussi $b = au^{-1}$ puis $a \mid b$ et $b \mid a$. Réciproquement, supposons $a|b$ et $b|a$. Si a est nul alors b est nul car $a|b$, et donc $a = b$. Sinon, on écrit $a = bc$ et $b = ad$ pour certains $c, d \in A$ puis $a = abd$, $a(1 - bd) = 0$ et $1 = bd$ par intégrité de A, *i.e.* $c, d \in A^\times$. □

Ces considérations montrent qu'il est important en pratique de savoir déterminer le groupe $A^\times$ des unités de A. Le cas de $\mathbb{Z}[\sqrt{d}]$ a déjà été traité.

EXEMPLE 2.4. *Si A est intègre, alors $A[X]$ l'est encore (on a $\deg PQ = \deg P + \deg Q$ pour $P, Q \neq 0$). On a aussi $A[X]^\times = A^\times$ (polynomes constants inversibles).*

Introduisons maintenant une première notion d'*irréductibilité*.

DÉFINITION 2.5. *Un élément non nul $\pi \in A$ est dit irréductible si ce n'est pas une unité, et si pour tout $a, b \in A$, la relation $\pi = ab$ implique $a \in A^\times$ ou $b \in A^\times$.*

Autrement dit, aux unités près un irréductible a exactement deux diviseurs : à savoir 1 et lui-même. Si π est irréductible, il en va de même de tout élément associé.

EXEMPLE 2.6. *Les irréductibles de $\mathbb{Z}$ sont les $\pm p$ avec p un nombre premier. Pour k un corps, les irréductibles de $k[X]$ (voire même de $k[X_1, \ldots, X_n]$) sont les polynômes irréductibles au sens usuel.*

Donnons quelques exemples et contre-exemples dans $\mathbb{Z}[\sqrt{d}]$. La multiplicativité de la norme N rendra bien des services pour étudier l'arithmétique de $\mathbb{Z}[\sqrt{d}]$, notamment car si a divise b dans $\mathbb{Z}[\sqrt{d}]$, alors $\mathrm{N}(a)$ divise $\mathrm{N}(b)$ dans $\mathbb{Z}$. (Mais la réciproque est très fausse !)

EXEMPLE 2.7. (i) Soit $\pi \in \mathbb{Z}[\sqrt{d}]$ avec $p = \mathrm{N}(\pi)$ irréductible dans $\mathbb{Z}$ (donc $\pm p$ premier). Alors π est irréductible dans $\mathbb{Z}[\sqrt{d}]$. Par exemple, $1 + 2i$ est

irréductible dans $\mathbb{Z}[i]$. En effet, si on a $\pi = ab$ on en déduit $\mathrm{N}(a) = \pm 1$ ou $\mathrm{N}(b) = \pm 1$ donc a ou $b \in \mathbb{Z}[\sqrt{d}]^\times$ (Lemme 1.4). La réciproque est fausse comme le montre l'exemple suivant.

(ii) Considérons $\mathbb{Z}[\sqrt{-3}]$ (d'unités ± 1). Comme $x^2 + 3y^2 = 2$ n'a pas de solution $(x, y) \in \mathbb{Z}^2$, il n'y a pas d'élément $a \in \mathbb{Z}[\sqrt{-3}]$ de norme ± 2. On en déduit que les éléments de norme 4 de $\mathbb{Z}[\sqrt{-3}]$ sont irréductibles : ce sont les 6 éléments $\pm 2, \pm(1 + \sqrt{3})$ et $\pm(1 - \sqrt{3})$.

Une notion concurrente à l'irréductibilité est la suivante.

Définition 2.8. *Un élément non nul $\pi \in A$ est dit premier si ce n'est pas une unité et s'il satisfait à la propriété d'Euclide-Gauss : pour tout $a, b \in A$, on a*

$$\pi \mid ab \implies \pi \mid a \text{ ou } \pi \mid b.$$

Exemple 2.9. (i) Un élément premier est irréductible. En effet, si $\pi = ab$ alors π divise a ou b. Si par exemple $\pi | a$, de sorte que $a = \pi c$ où $c \in A$, alors $\pi = \pi cb$ puis $1 = cb$, et donc b est une unité.

(ii) La réciproque est vraie dans $\mathbb{Z}$ ou $k[X]$ avec k un corps, mais pas en général. En effet, l'élément 2 est irréductible dans $\mathbb{Z}[\sqrt{-3}]$ comme on l'a vu. Il ne divise pas $1 \pm \sqrt{-3}$, car sinon on aurait $1 \pm \sqrt{-3} = 2(x + y\sqrt{-3}) = 2x + 2y\sqrt{-3}$ et donc $2x = \pm 1$ et $2y = \pm 1$ avec $x, y \in \mathbb{Z}$: absurde. Pourtant il divise $2.2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$: il n'est pas premier.

3. Anneaux factoriels

On note toujours A un anneau commutatif intègre. On convient qu'un produit indexé par l'ensemble vide dans un anneau vaut 1, et aussi que l'on a $a^0 = 1$ pour tout $a \in A$. Il sera commode pour la suite de choisir un ensemble (arbitraire) $\mathscr{P}$ de représentants des éléments irréductibles pour la relation d'association. Dans le cas $A = \mathbb{Z}$ (d'unités ± 1), le choix classique est de prendre l'ensemble des nombres premiers positifs ! De même un choix standard dans le cas $A = k[X]$ est celui des polynômes irréductibles *unitaires*. On note $\mathbb{N}^{(\mathscr{P})}$ l'ensemble des familles $(n_\pi)_{\pi \in \mathscr{P}}$ telles que $\{\pi |\, n_\pi \neq 0\}$ est fini. La définition suivante, abstraction du *théorème fondamental de l'arithmétique*, est importante.

Définition 3.1. *(i) On dit que A a la* propriété de factorisation (notée (PF)) *si tout élément de $A \setminus \{0\}$ est un produit fini (éventuellement vide) d'éléments irréductibles et d'une unité.*

(ii) On dit que A est factoriel *si pour tout $a \in A \setminus \{0\}$ il existe un unique $u \in A^\times$ et une unique élément $(v_\pi(a)) \in \mathbb{N}^{(\mathscr{P})}$ vérifiant $a = u \prod_{\pi \in P} \pi^{v_\pi(a)}$.*

Le sens donné au produit ci-dessus est bien entendu le produit fini de u et des $\pi^{v_\pi(a)}$ avec $v_\pi(a) \neq 0$, mais il est commode de le noter ainsi. Il est facile de voir que la propriété d'être factoriel ne dépend pas du choix de l'ensemble de représentants $\mathscr{P}$ des irréductibles de A.

Exemple 3.2. (i) *Les anneaux $\mathbb{Z}$ et $k[X]$ avec k un corps sont factoriels*, nous le redémontrerons plus loin.

(ii) Les anneaux $\mathbb{Z}[\sqrt{d}]$ sont (PF). En effet, vérifions par récurrence sur l'entier $|\mathrm{N}(a)| \geqslant 1$ que tout $a \in A$ non nul est produit fini d'irréductibles et d'une unité. Si a est une unité, *i.e.* $|\mathrm{N}(a)| = 1$ par le Lemme 1.4, ou irréductible, il y a rien à démontrer. Sinon, on a $a = bc$ avec $1 < |\mathrm{N}(b)|, |\mathrm{N}(c)| < |\mathrm{N}(a)|$ toujours par le Lemme 1.4. Ainsi, b et c sont produits finis d'irréductibles, ainsi donc que $a = bc$.

(iii) *L'anneau* $\mathbb{Z}[\sqrt{-3}]$ *n'est pas factoriel* : on a $2.2 = (1-\sqrt{-3})(1+\sqrt{-3})$ alors que $2, 1+\sqrt{-3}$ et $1-\sqrt{-3}$ sont irréductibles deux à deux non associés (Exemple 2.7).

(iv) *L'anneau* $\mathrm{H}(\mathbb{C})$ *des séries entières convergentes sur* $\mathbb{C}$ *est intègre*, par le principe des zéros isolés. On peut montrer que *les unités de* $\mathrm{H}(\mathbb{C})$ *sont exactement les fonctions qui ne s'annulent pas sur* $\mathbb{C}$*, et ses irréductibles sont les associés des* $z-a$ *avec* $a \in \mathbb{C}$. Mais certains éléments de $\mathrm{H}(\mathbb{C})$ ont une infinité de 0, comme par exemple $\sin(\pi z)$, donc *l'anneau* $\mathrm{H}(\mathbb{C})$ *ne vérifie pas* (PF) (voir l'Exercice 7.21).

L'arithmétique des anneaux factoriels est particulièrement simple. En effet, supposons A factoriel. Pour $a \in A$ non nul et $\pi \in \mathscr{P}$, l'entier $v_\pi(a) \in \mathbb{N}$ est appelée *valuation de* a *en* π, ou *valuation* π-adique de a. La factorialité impose que pour tout $a, b \in A\backslash\{0\}$ et tout $\pi \in \mathscr{P}$, on a $v_\pi(ab) = v_\pi(a) + v_\pi(b)$. En particulier, on a

$$a \mid b \Leftrightarrow \quad \forall \pi \in \mathscr{P},\ v_\pi(a) \leqslant v_\pi(b). \tag{59}$$

Proposition 3.3. (Caractérisation d'Euclide-Gauss des anneaux factoriels). *Supposons que* A *satisfait* (PF)*. Alors* A *est factoriel si, et seulement si, tout irréductible de* A *est premier.*

Démonstration — Supposons A factoriel. Soit π un irréductible de A, que l'on peut supposer dans $\mathscr{P}$. Si π divise ab, alors $1 \leqslant v_\pi(ab) = v_\pi(a) + v_\pi(b)$ et donc soit $v_\pi(a) \geqslant 1$ soit $v_\pi(b) \geqslant 1$. Ainsi, π est premier.

Supposons réciproquement que tout irréductible de A est premier et montrons A factoriel. Supposons que l'on ait $u, v \in A^\times$ et $(m_\pi), (n_\pi) \in \mathbb{N}^{(\mathscr{P})}$ avec

$$u \prod_{\pi \in \mathscr{P}} \pi^{m_\pi} = v \prod_{\pi \in \mathscr{P}} \pi^{n_\pi}, \tag{60}$$

Montrons $u = v$ et $(m_\pi) = (n_\pi)$ par récurrence sur $\sum_\pi (m_\pi + n_\pi)$. C'est clair si cette somme est nulle. Supposons par exemple $m_\pi \geqslant 1$. Alors π divise le membre de gauche de (60), et donc celui de droite. De plus, π ne divise pas d'unité car on a $\pi \notin A^\times$. Comme π est premier, il divise donc $\pi'^{n_{\pi'}}$ pour un certain $\pi' \in \mathscr{P}$ avec $n_{\pi'} \geqslant 1$, et en particulier π divise π'. Comme π' est irréductible cela implique $\pi \sim \pi'$ puis $\pi' = \pi$ par définition de $\mathscr{P}$, et donc $n_\pi \geqslant 1$. Par intégrité, on peut donc diviser par π des deux côtés l'Équation (60), et on conclut par récurrence. □

Remarque 3.4. *À l'aide de la notion de contenu d'un polynôme, on peut montrer que si* A *est factoriel, alors* $A[X]$ *est factoriel (un argument connu de Gauss) : voir l'Exercice 7.20.*

Terminons par une discussion de la notion de pgcd et ppcm.

DÉFINITION 3.5. *Soient $a_1, \dots, a_n \in A$, on appelle plus grand diviseur commun (ou pgcd) des a_i un élément $d \in A$ vérifiant les deux propriétés suivantes :*

(i) d divise a_i pour tout i,

(ii) pour tout $b \in A$, si b divise a_i pour tout i alors b divise d.

Autrement dit, c'est "le" plus grand élément de l'ensemble des éléments inférieurs aux a_i pour la relation de divisibilité. Observons que s'ils existent, *deux pgcd se divisent entre eux, et sont donc associés.* En revanche, les pgcds n'existent pas toujours, même si les a_i ne sont pas tous nuls (voir les exercices). On définit de même la notion de *plus petit multiple commun* (ou ppcm) des a_i comme étant un plus petit élément de l'ensemble des éléments plus grands que les a_i pour la relation de divisibilité (les même remarques s'appliquent).

LEMME 3.6. *Pgcd et ppcm existent dans un anneau factoriel.*

DÉMONSTRATION — En effet, un pgcd de $a_1, \dots, a_n \in A \smallsetminus \{0\}$ est $\prod_{\pi \in \mathscr{P}} \pi^{m_\pi}$ avec $m_\pi = \mathrm{Min}\{\mathrm{v}_\pi(a_1), \dots, \mathrm{v}_\pi(a_n)\}$. Un ppcm s'obtient de même en remplaçant le Min par un Max. □

Terminons par la notion d'éléments premiers entre eux.

DÉFINITION 3.7. *Les éléments $a_1, \dots, a_n \in A$ sont dits premiers entre eux si leurs seuls diviseurs communs sont les unités : pour tout $d \in A$ on a $d \,|\, a_i \ \ \forall i \implies d \in A^\times$.*

Il est équivalent de dire que 1 en est un pgcd.

4. Idéaux

Dans cette section, A désigne un anneau commutatif[1] quelconque.

DÉFINITION 4.1. *Un idéal de A est un sous-groupe additif $I \subset A$ tel que pour tout $a \in A$ et tout $x \in I$ on ait $ax \in I$.*

L'ensemble $aA = \{ax \,|\, x \in A\}$ des multiples de a dans A est un idéal appelé *idéal principal engendré par $a \in A$*. On note aussi $(a) = aA$. En particulier, *l'idéal nul* $\{0\}$ et *l'idéal total* A sont des idéaux de A. De plus, la divisibilité entre éléments s'exprime simplement en terme des idéaux principaux associés : pour $a, b \in A$ on a

$$bA \subset aA \iff b \in aA \iff a|b$$

La devise à retenir est "contenir c'est diviser". En particulier, on a $aA = A \iff a \in A^\times$, et $aA = bA \iff a \sim b$.

REMARQUE 4.2. (*Nombres idéaux de Kummer*) La terminologie *idéal*, introduite par Dedekind, est empruntée à celle de *nombres idéaux* utilisée par Kummer dans son étude des anneaux de la forme $\mathbb{Z}[e^{2i\pi/n}]$. Suivant Kummer, on peut penser à un idéal de A comme une partie qui satisfait axiomatiquement tout pour être l'ensemble des multiples de "quelque chose", mais que ce "quelque chose" n'est pas forcément

1. La condition de commutativité de A n'est pas cruciale, mais sans elle il conviendrait de distinguer les notions d'idéal à gauche, idéal à droite, et idéal bilatère. Cette généralité est hors de propos ici, mais d'un grand intérêt dans d'autres situations.