Arithmétique des anneaux principaux

Résumé

Nous nous intéressons plus généralement à la généralisation de l'arithmétique de $\mathbb{Z}$, très naturelle, dans les anneaux commutatifs, à l'aide d'un formalisme épuré grâce à la notion d'idéal. On s'aperçoit que l'arithmétique des anneaux s'assimile d'autant plus à celle des entiers lorsque que l'on renforce les hypothèses sur l'anneau considéré : intégrité en premier lieu, puis factorialité, principalité, et enfin présence d'une division euclidienne. Dans cette construction, les anneaux principaux ont un rôle crucial : s'ils généralisent les anneaux euclidiens, on montre que les anneaux principaux sont tous factoriels, c'est-à-dire qu'ils admettent un théorème fondamental de l'arithmétique ; c'est ainsi dans la structure d'anneau principal que l'arithmétique devient significativement plus manipulable. Nous verrons enfin l'application de cette arithmétique dans la résolution d'équations diophantiennes cas particuliers de la grande équation de Fermat.

1 Préliminaires

One Ring to rule them all, One Ring to find them, One Ring to bring them all and in the darkness bind them.

J. R. R. Tolkien, *The Fellowship of the Ring*

1.1 Notions générales sur les anneaux

Nous ne nous intéressons qu'aux anneaux unitaires (de même que, très vite, nous ne nous intéressons qu'aux anneaux commutatifs). En effet, dans un pseudo-anneau, nous ne disposons pas du lemme de la partie **1.2**, ni de la caractérisation de l'association dans la partie **1.3**.

Définition. ***(Anneau)***

Un anneau $(A, +, \times)$ est la donnée d'un groupe commutatif $(A, +)$ et d'une loi de composition interne $\times$ sur A associative, possédant un élément neutre et distributive à gauche et à droite sur $+$.

Définition. ***(Intégrité)***

Un anneau est dit *intègre* s'il est commutatif et sans diviseur de zéro autre que zéro lui-même. Autrement dit, A est commutatif et pour tous $a, b \in A$, $ab = 0$ si et seulement si $a = 0$ ou $b = 0$.

Définition. ***(Unités)***

On note A^* ou $A^\times$ l'ensemble des *unités* ou *inversibles* de A, c'est-à-dire l'ensemble des éléments symétrisables pour la loi $\times$ dans A.

1.2 Idéaux

1.2.1 Définition

Définition. ***(Idéal)***

Soit A un anneau unitaire et I une partie de A. On dit que I est un *idéal à gauche* de A si $(I,+)$ est un sous-groupe de $(A,+)$ et pour tous $a \in A$, $x \in I$, on a $ax \in I$. On définit de même un *idéal à droite* de A. Si I est un idéal de A à gauche et à droite, on dit que I est un idéal *bilatère*. Dans un anneau commutatif, les notions d'idéal à droite et d'idéal à gauche sont confondues.

Propriété. ***(Intersection d'idéaux)***

Toute intersection d'idéaux à gauche (resp. à droite, bilatères) est un idéal à gauche (resp. à droite, bilatère). C'est le plus grand idéal contenu dans tous ceux-là.

Propriété. ***(Somme d'idéaux)***

Toute somme finie d'idéaux à gauche (resp. à droite, bilatères) est un idéal à gauche (resp. à droite, bilatère). C'est le plus petit idéal contenant tous ceux-là.

1.2.2 Idéal principal engendré par un élément

Définition-propriété. ***(Idéal principal engendré par un élément)***

Soit $a \in A$. Alors aA est un idéal à droite de A, appelé *idéal à droite principal de A engendré par a*. On dit aussi que a est UN *générateur* de aA. On note $aA = (a)_d$. Un idéal est dit *principal* s'il est l'idéal principal engendré par un des éléments de A. On définit de même l'idéal à gauche principal engendré par a noté $(a)_g$, l'idéal bilatère engendré par a noté $(a) = AaA$ et dans le cas commutatif, $aA = Aa$ donc on parle d'idéal principal engendré par un élément et l'on note (a).

▷ Simple vérification. ■

Voilà maintenant un lemme élémentaire, mais fort utile.

Lemme

Soit A un anneau unitaire, I un idéal à gauche (resp. à droite, bilatère) de A.

1. On a $I = A$ si et seulement si $I \cap A^* \neq \emptyset$.
2. Si A est de plus commutatif, pour tout $a \in A$, $(a) = A$ si et seulement si a est une unité.

▷ Pour le premier point, si $I = A$, I contient 1_A qui est inversible. Réciproquement, supposons que I contient $u \in A^*$. Alors pour tout $a \in A$, $a = (au^{-1})u \in I$, car I est un idéal à gauche, donc

$A \subseteq I$, donc $I = A$ (les démonstrations pour les idéaux à droite et bilatères sont identiques).

Pour le second point, on suppose A commutatif. Soit $a \in A$. Si a est inversible, alors $(a) = A$ par le point précédent. Inversement, si $(a) = A$, alors $1_A \in A$, donc il existe $b \in A$ tel que $ba = 1_A$. Ainsi, $a \in A^*$, car $ab = ba = 1_A$. ■

Corollaire

Soit A un anneau. Alors A est un corps (non nécessairement commutatif) si et seulement s'il possède exactement deux idéaux à gauche, à savoir $\{0_A\}$ et A.

▷ Soit A un corps, non nécessairement commutatif. $0_A \neq I_A$, car un corps, par axiome, n'est jamais trivial, donc $\{0_A\}$ et A sont deux idéaux à gauche de A distincts. Soit I un idéal à gauche de A. S'il est non nul, il contient un élément non nul, donc inversible puisque A est un corps, et donc égal à A par le lemme précédent. Réciproquement, supposons que $\{0_A\}$ et A soient les deux seuls idéaux à gauche de A. Puisqu'ils sont distincts, $0_A \neq 1_A$ donc A n'est pas trivial. Soit $a \in A \setminus \{0_A\}$. Alors $(a)_g$ est un idéal à gauche de A non nul, car il contient a, car A est unitaire, et comme $1_A \in A$, il existe $b \in A$ tel que $ba = 1_A$. Remarquons que b est non nul, car 0_A est absorbant et l'on aurait encore $0_A = 1_A$. Par le même raisonnement, il existe $c \in A$ tel que $cb = 1_A$. On a lors $a = 1_A a = (cb)a = c(ba) = c1_A = c$, donc $ab = 1_A$ par substitution. Ainsi a est inversible. Donc, A est un corps. ■

1.2.3 Idéaux maximaux, idéaux premiers

Définition. *(Idéal propre)*

Un idéal I de A est *propre* si $I \neq A$.

Définition. *(Idéal maximal)*

Un idéal I de A est dit *maximal* s'il est élément maximal[a] pour l'inclusion parmi les idéaux propres de A.

[a] Un élément a d'un espace ordonnée $(E, \leq)$ est dit *maximal* si pour tout $x \in E$, $a \leq x \Rightarrow x = a$.

Propriétés

- L'idéal I est maximal si et seulement si I est propre et pour tout $x \in A \setminus I$, $I + Ax = A$.
- L'idéal I est maximal si et seulement si A/I est un corps (non nécessairement commutatif).

▷ Si I est maximal, pour tout $x \in A \setminus I$, $I + Ax$ est un idéal contenant strictement I, donc par maximalité, il égale A. Soit maintenant $\overline{x}$ un élément non nul de l'anneau quotient A/I. Cela signifie que $x \notin I$, et, par hypothèse, il existe $a \in A$ et $i \in I$ tel que $i + ax = 1$, ce qui entraîne $\overline{ax} = 1$ dans A/I, donc tout élément non nul de A/I est inversible. Puisque I est propre, A/I est non trivial ; A/I est donc un corps non nécessairement commutatif. Si l'on suppose cela, enfin, ses seuls idéaux

sont triviaux. Or le théorème de correspondance (donnant les sous-groupes distingués d'un groupe quotient) énonce que l'existence d'une bijection entre les idéaux de A contenant I et les idéaux de A/I : le seul idéal propre de A contenant I est donc lui-même, ce qui signifie que I est maximal parmi les idéaux propres de A. Toutes ses propositions sont donc équivalentes. ■

Théorème. ***(Krull, 1929)***

Tout idéal propre d'un anneau A est inclus dans un idéal maximal de A.

▷ C'est une conséquence directe du lemme de Zorn appliqué à l'ensemble des idéaux propres de A contenant I, qui est clairement inductif. Nous montrons donc le lemme de Zorn.

Nous donnons une preuve plutôt laborieuse de ce résultat, dite « par au-dessus » (*top-down* en anglais). Celle-ci est beaucoup moins judicieuse qu'une preuve « par en dessous » (*bottom-up* en anglais), qui est l'autre preuve classique du lemme de Zorn, mais a l'avantage de ne pas recourir à la théorie des ordinaux.

Soit $(E, \leqslant)$ un ensemble ordonné inductif. Remarquons que l'ensemble vide n'est pas inductif. Soit σ une fonction de choix sur la famille de toutes les parties non vides de E. Pour $X \subseteq E$ et $a \in E$, on note $X \preccurlyeq a$ pour $\forall x \in X, x \leqslant a$ et de même pour une inégalité stricte. Pour toute chaîne C, on définit $C^+ = C \cup \{\sigma(\{a \mid C \prec a\})\}$ si $\{a \mid C \prec a\}$ est non vide, et $C^+ = C$ sinon.

Soit C une chaîne quelconque de E (il en existe toujours une, par exemple la partie vide). Parce que E est inductif, il existe a vérifiant $C \preccurlyeq a$ par définition. Si a est maximal dans E, il n'y a rien à faire. Sinon, par définition, il existe un certain b dans E vérifiant $a < b$, et donc par transitivité $C \prec b$. Par conséquent, si C est une chaîne telle que $\{a \mid C \prec a\}$ soit vide, c'est-à-dire vérifiant $C^+ = C$, alors il existe une élément maximal dans E. Nous allons construire une telle chaîne.

On appelle *close* toute famille K de chaînes de E telle que $C \in K$ entraîne $C^+ \in K$, et que, si J est une partie de K formées de chaînes deux à deux comparables pour l'inclusion, alors leur réunion appartienne encore à K. La famille de toutes les chaînes de A est évidemment close, et l'on vérifie que toute intersection de familles closes est close. Il existe donc une plus petite famille close K (l'intersection de toutes les familles closes, qui ne pose pas de problème de définition puisque l'ensemble des familles closes est non vide). Posons enfin $K' = \{C \in K \mid \forall D \in K,\ C \subseteq D \vee D \subseteq C\}$. On va montrer que $K' = K$, c'est-à-dire que K est composée de chaînes deux à deux comparables pour l'inclusion. Supposons cela démontré. On pose C la réunion des éléments de K. Par définition, on a $C \in K$ et donc $C^+ \in K$. Or, par construction, on a $D \subseteq \bigcup K = C$ pour toute chaîne D dans K. En particulier, on a donc $C^+ \subseteq C$, d'où $C^+ = C$, comme souhaité.

Revenons sur notre postulat. Puisque K est la plus petite famille close, et que l'on a $K' \subseteq K$, il suffit, pour montrer $K' = K$, de montrer que K' est close. Soit $C \in K'$. Posons $K_C = \{D \in K \mid D \subseteq C \vee C^+ \subseteq K'\}$. Supposons que $D \in K_C$. Si $C^+ \subseteq D$, on a *a fortiori* $C^+ \subseteq D^+$. Pour $C = D$, on a trivialement $C^+ = D^+$. Supposons alors $D \subsetneq C$. Par hypothèse, D^+ est dans K, et C est dans K', donc on a $D^+ \subseteq C$ ou $C \subsetneq D^+$. Le second cas est incompatible avec $D \subsetneq C$ puisque D^+ privé de D est un singleton. Dans tous les cas, $D \in K_C$ entraîne donc $D^+ \in K_C$. Supposons maintenant que J soit un sous-ensemble de K_C formé de chaînes deux à deux comparables pour l'inclusion. Ou bien on

a $D \subseteq C$ pour tout D dans J, et l'on a alors $\bigcup J \subseteq C$, ou bien il existe D dans J vérifiant $C^+ \subseteq D$, et l'on a alors $C^+ \subseteq \bigcup J$: dans les deux cas, $\bigcup J$ est dans K_C. Ainsi, K_C est une famille close, donc $K_C = K$, ce qui montre que C^+ est dans K' dès que C s'y trouve.

Finalement, supposons que J est un sous-ensemble de K' formé de chaînes deux à deux comparables pour l'inclusion. Soit D une chaîne quelconque dans K. Ou bien on a $C \subseteq D$ pour toute chaîne C dans J, dont on déduit que $\bigcup J \subseteq D$, ou bien il existe C dans J vérifiant $D \subseteq C$, dont on déduit que $D \subseteq \bigcup J$. Donc, dans tous les cas, $\bigcup J \in K'$. Il en résulte que K' est close, et on a donc $K' = K$. ■

Définition. ***(Idéal premier)***

On appelle *idéal premier* de A tout idéal I tel que l'anneau quotient A/I est intègre.

Propriété

Un idéal I est premier si et seulement si pour tous $x, y \in A$, si $xy \in I$, $x \in I$ ou $y \in I$.

▷ Notons $\overline{x}$ la classe de $x \in A$ dans A/I. Alors $\overline{x} = 0 \Leftrightarrow x \in I$ et tous les éléments de A/I sont de la forme $\overline{x}$, $x \in A$. L'implication de la définition se réécrit donc $\forall \overline{x}, \overline{y} \in A/I$, $\overline{xy} \Rightarrow (\overline{x} = 0$ ou $\overline{y} = 0)$, ce qui caractérise l'intégrité de A/I. ■

Corollaire

Tout idéal maximal est premier.

▷ Tout corps est intègre. ■

Corollaire

Tout anneau admet des idéaux premiers.

▷ Conséquence directe de la définition précédente et du théorème de Krull. ■

1.3 Divisibilité dans un anneau

1.3.1 Division et association

Définition. ***(Divisibilité)***

Soient $a, b \in A$. On dit que a *divise* b, ou que a est un *diviseur* de b, ou que b est un *multiple* de a, si b appartient à l'idéal principal à gauche engendré par a, c'est-à-dire, s'il existe $c \in A$ tel que $b = ac$. On note : $a|b$.

Remarque. Cela correspond bien à la définition de la divisibilité dans $\mathbb{Z}$ apprise dans les petites classes. Cependant remarquons : dans un anneau quelconque, l'élément 0 est absorbant. On en déduit que tout élément divise 0, mais que 0 ne divise que lui-même.

On prendra garde au fait suivant : la notion de divisibilité est intrinsèque à l'anneau ambiant. Ainsi 2 divise 3 dans $\mathbb{Q}$, car $3 = 2.\frac{3}{2}$, mais 2 ne divise pas 3 dans $\mathbb{Z}$.

Propriété. ***(Définition équivalente de la divisibilité)***

Soient $a, b \in A$. L'élément a divise b, si et seulement si, $bA \subseteq aA$.

▷ Supposons que $bA \subseteq aA$. L'élément b est inclus dans bA, car $b = b1_A$, A étant unitaire. Donc $b \in aA$, autrement dit, b est dans l'idéal principal engendré par a, ce qui signifie exactement que a divise b. Réciproquement, si a divise b, il existe $c \in A$ tel que $b = ac$. Soit $x \in bA$: $x = bu$ pour un certain $u \in A$. Alors $x = acu$, car $b = ac$. En posant $y = cu$, $x = ay$ pour $y \in A$ stable par multiplication. Donc $x \in aA$, donc $bA \subseteq aA$. ■

Attention à ne pas inverser le sens de l'inclusion dans $bA \subseteq aA$!

Propriété. ***(Préordre de divisibilité)***

La relation de divisibilité dans un anneau est réflexive et transitive.

▷ Ces deux propriétés sont héritées de l'ordre $\subseteq$ et de la propriété précédente. ■

Définition. ***(Éléments associés)***

Deux éléments $a, b \in A$ sont dits *associés* si $a|b$ et $b|a$ (autrement dit, si $aA = bA$).

Remarques.

1. Deux éléments associés ne sont pas nécessairement égaux (voir l'exemple ci-dessous).
2. Si cette propriété est vérifiée, alors la divisibilité est un ordre sur A, comme le remarque le fait ci-dessous. Ce n'est pas le cas dans $\mathbb{Z}$: deux éléments associés sont opposés. Si l'on se restreint à $\mathbb{N}$ (qui n'est pas un anneau !), la relation de divisibilité est donc un ordre.
3. Dans $\mathbb{K}[X]$, pour un corps $\mathbb{K}$, les éléments associés à un polynôme P sont les λP pour $\lambda \in \mathbb{K} \setminus \{0\}$. En particulier, tout polynôme non nul est associé à un unique polynôme unitaire de même degré.

On se place dès à présent dans des anneaux **commutatifs**.

Propriété. ***(Caractérisation de l'association dans les anneaux intègres)***

Deux éléments d'un anneau **intègre** sont associés s'il existe une unité $c \in A^*$ telle que $b = ac$, cette relation étant bien sûr symétrique.

▷ Soient $a, b \in A$. On a successivement :

$$\begin{aligned} aA = bA &\Leftrightarrow \begin{cases} aA \subseteq bA \\ bA \subseteq aA \end{cases} \\ &\Leftrightarrow \begin{cases} a = bc, c \in A \\ b = ac', c' \in A \end{cases} \\ &\Leftrightarrow \begin{cases} a = bc, c \in A \\ b = bcc', c' \in A \end{cases} \\ &\Leftrightarrow \begin{cases} a = bc, c \in A \\ cc' = 1, c' \in A \end{cases} \\ &\Leftrightarrow a = bc, c \in A^*, \end{aligned}$$

l'avant-dernière équivalence n'ayant lieu que par ce que b est régulier dans A, car A est intègre. ■

Remarque. Dans un anneau commutatif quelconque, deux éléments égaux à un inversible près sont clairement associés. En revanche, si l'anneau A n'est pas intègre, deux éléments peuvent être associés sans être égaux à un inversible près, mais il est très délicat d'exhiber un contre-exemple (il s'agit d'étudier les inversibles de l'anneau $\mathbb{Z}[X, Y, Z]/(X(1 - YZ))$).

Proposition

L'association $\mathcal{A}$ est une relation d'équivalence.

Fait

Pour tout anneau unitaire A, la divisibilité est un ordre sur $A/\mathcal{A}$.

Propriété. ***(Combinaison linéaire)***

Si a divise b et c, alors pour tous m, n, a divise $bm + cn$.

▷ Par hypothèse, $ak = b$ et $aq = c$. Ainsi $akm = bm$ et $aqn = cn$, d'où $akm + aqn = a(km + qn) = bm + cn$ par distributivité, donc, comme $km + qn \in A$, a divise $bm + cn$. ■

1.3.2 Primalité relative et étrangeté

Définition. ***(Primalité relative)***

On dit que $a, b \in A$ sont *premiers entre eux*, ou que a est *premier à* b, si pour tout $d \in A$, on a $(d|a \text{ et } d|b) \Rightarrow d \in A^*$.

Définition. ***(Étrangeté)***

On dit que $a, b \in A$ sont *étrangers*, s'il existe $u, v \in A$ tels que $au + bv = 1$.

Note générale

Plus généralement, on peut définir dans un anneau A les trois concepts suivants :

- deux éléments $a, b \in A$ sont *premiers entre eux* si $(a) + (b)$ n'est inclus dans aucun idéal principal propre (ou, ce qui revient au même, si $1 \in pgcd(a, b)$) ;
- deux éléments sont *indissolubles* si b est simplifiable dans $A/(a)$ (ou, ce qui revient au même, si $ab \in ppcm(a, b)$) ;
- deux éléments sont *étrangers* lorsque $(a) + (b) = A$ (ou, ce qui revient au même, si les idéaux (a) et (b) sont étrangers.

On a les implications strictes : étrangers $\Rightarrow$ indissolubles entre eux $\Rightarrow$ premiers entre eux. (Les réciproques peuvent être fausses même dans un anneau intègre.)

Propriété

Deux éléments étrangers sont premiers entre eux.

▷ Soient a, b étrangers. Il existe donc $u, v \in A$ tels que $ua+vb = 1$. Soit $d \in A$ tel que d divise a et b. Alors d divise la combinaison linéaire $ua + vb$, c'est-à-dire d divise 1. Ceci signifie exactement, dans un anneau commutatif, que d est inversible. ■

1.3.3 Pgcd et ppcm

Définition. ***(Plus grand commun diviseur)***

Soient $a, b \in A$. On dit que $d \in A$ est UN *plus grand diviseur commun*, ou *pgcd*, de a et b, si d divise a et b et pour tout $c \in A$, si c divise a et b, c divise d.

Définition. ***(Plus petit commun multiple)***

Soient $a, b \in A$. On dit que $m \in A$ est UN *plus grand multiple commun*, ou *ppcm*, de a et b, si a et b divisent m et pour tout $c \in A$, si a et b divisent c, m divise c.

Remarques.

1. Pgcd et ppcm n'existent pas toujours. Par exemple, si $A = \mathbb{Z}[i\sqrt{5}]$, on peut montrer que 9 et $3(2 + i\sqrt{5})$ n'ont pas de pgcd et que 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm.
2. Le pgcd et le pcpm ne sont pas forcément unique (voir par exemple dans $\mathbb{R}[X]$), mais la proposition suivante permet d'y voir nettement plus clair.
3. Si $a = 0$, b est un pgcd de $a$et b. En particulier, $pgcd(0, 0) = 0$. Si $(a, b) \neq (0, 0)$, un pgcd de a et b est non nul.
4. Si $a = 0$ ou $b = 0$, 0 est un ppcm de a et b. De plus, c'est le seul. Si a et b sont non nuls, un ppcm m de a et b est non nul dès que A est intègre, puisque m divise ab, qui est non nul.

Lemme. ***(Unicité essentielle du pgcd et du ppcm)***

Deux pgcd (resp. ppcm) de deux éléments d'un anneau A, lorsqu'ils existent, sont uniques à association près.

▷ On le montre pour le pgcd, le cas du ppcm étant similaire. Supposons que d et d' soient deux pgcd de a et b. Alors, puisque d' est un pgcd de a et b et que d est un diviseur commun à a et b, on a $d|d'$. Symétriquement, $d|d'$; autrement dit, d et d' sont associés. ■

1.3.4 Irréductibilité, primalité

Définition. ***(Irréductible)***

Un élément $\pi \in A$ est dit *irréductible* s'il est non nul, non inversible, et si pour tous $a, b \in A$, on a $\pi = ab \Longrightarrow a \in A^*$ ou $b \in A^*$.

Remarques.

1. Cela revient à dire que π est non nul, non inversible, et que ses seuls diviseurs sont les éléments $u \in A^*$ et $v\pi$, $v \in A^*$. Ceux-ci sont toujours diviseurs, puisque l'on peut écrire $a = u(u^{-1}a) = (va)v^{-1}$.
2. Si a et b sont deux éléments de A associés, alors a est irréductible dans A si et seulement si b l'est. Dans ce cas, on a nécessairement $b = ua$ avec $u \in A^*$. En effet, supposons a et b associés, soit $(a) = (b)$. Supposons également que a soit irréductible. Comme a est non nul et non inversible, (a) est non nul et distinct de A. Il en est donc de même de (b), et b est alors non nul et non inversible. Puisque $a \in (a) = (b)$, il existe $c \in A$ tel que $a = bc$. Puisque b est non inversible et a est irréductible, on a $c \in A^*$. Enfin, si π est irréductible et $u \in A^*$, alors $u\pi$ est irréductible. En effet, si $u\pi = ab$, alors $\pi = (u^{-1}a)b$. Ainsi, b est inversible ou $u^{-1}a$ est inversible, mais cette dernière condition est équivalente à ce que a soit inversible, car si $u^{-1}a = v$ inversible, $a = uv$ est inversible et si a est inversible, $u^{-1}a$ l'est comme produit d'inversibles.

Dans $\mathbb{Z}[i\sqrt{3}]$, les éléments $1\pm i\sqrt{3}$ sont irréductibles mais non associés (voir la suite).

3. Un anneau ne possède pas nécessairement d'éléments irréductibles. C'est le cas des corps, ou par exemple de $\mathbb{Z}/6\mathbb{Z}$. En effet, il suffit d'écrire $4 = 2 \times 2$, $2 = 2 \times 4$, et $3 = 3 \times 3$.

4. Les irréductibles de $\mathbb{Z}$ sont les $\pm p$ où p est un nombre premier. Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Exemple fondamental

On considère l'anneau $A = \mathbb{Z}[i\sqrt{3}]$ des polynômes en $i\sqrt{3}$ à coefficients dans $\mathbb{Z}$. Montrons que les éléments 2 et $1 \pm i\sqrt{3}$ sont irréductibles non associés deux à deux.
Remarquons tout d'abord que si $z \in A$, il est inversible, si et seulement si $z \in \mathbb{U}$.
En effet, si $|z| = 1$, alors $|z^2| = z\overline{z} = 1$, et comme $\overline{z} \in A$, z est inversible.
Inversement, si z est inversible, il existe $z' \in A$ tel que $zz' = 1$, et donc $|z|^2|z'|^2 = 1$. Comme ces deux quantités sont des entiers positifs, on en déduit en particulier que $|z|^2 = 1$, donc $|z| = 1$.
Déterminons A^*. Par ce qui précède, $z = a + ib\sqrt{3}$ est inversible, si et seulement si, $a^2 + 3b^2 = 1$. Nécessairement, on a $b = 0$, ce qui implique $a = \pm 1$. Réciproquement 1 et -1 sont inversibles. Par conséquent, $A^* = \{\pm 1\}$.
Supposons enfin que z soit égal à 2, $1 + i\sqrt{3}$ ou $1 - i\sqrt{3}$.
Alors on a dans les trois cas $|z|^2 = 4$, donc z est non nul et non inversible par le point précédent. De plus, si $z = z_1 z_2$, $z_1, z_2 \in A$, alors $|z_1|$ divise 4. On a donc $|z_1| = 1, 2$ ou 4. Dans le premier cas, $z_1 \in A^*$ et dans le dernier, $z_2 \in A^*$.
Supposons que $|z_1| = 2$. C'est impossible : si $z_1 = a + bi\sqrt{3}$, $a^2 + 3b^2 = 2$ d'où $b = 0$ puis $a^2 = 2$. Ainsi, ces trois éléments sont irréductibles.
Il est immédiat qu'ils sont associés puisque les inversibles de A sont ± 1.

Propriété

Deux irréductibles non associés sont premiers entre eux.

▷ Soient π, π' deux éléments irréductibles de A. Soient $d \in A$ tel que $d|\pi$ et $d|\pi'$. Il existe donc des éléments b, b' tels que $db = \pi$ et $db' = \pi'$. Puisque π est irréductible, d est inversible ou b est inversible. Supposons que b soit inversible. Alors $d = b^{-1}\pi$ et $\pi' = (b^{-1}b)'\pi$. Comme π est irréductible, π est non inversible par définition. Mais, π' étant un élément irréductible, on en déduit que l'on a $u = b^{-1}b' \in A^*$. En particulier, π et π' sont associés, ce qui est contredit l'hypothèse. Ainsi, $d \in A^*$, ce que l'on voulait vérifier. ■

On dispose du lemme suivant donnant une condition suffisante pour qu'un élément d'un anneau intègre soit irréductible.

Lemme

Soient A un anneau, $\pi \in A$.

1. L'idéal (π) est premier non nul si et seulement si π est non nul, non inversible et vérifie le lemme d'Euclide : pour tous $a, b \in A$, π divise ab si et seulement si π divise a ou π divise b.
2. Si A est intègre, et si π vérifie l'une des deux conditions équivalentes précédentes, alors π est irréductible.

▷ Montrons le lemme point par point.

1. Supposons que $(\pi) = \pi A = A\pi$ soit premier non nul. Alors π est non nul, car πA ne l'est pas, et non inversible, car sinon, $\pi A = A$ et $A/(\pi)$ est non trivial, car il est intègre, car (π) est premier. Soient $a, b \in A$ tels que π divise ab. Par définition, $ab \in (\pi)$. Puisque (π) est un idéal premier, on a $a \in (\pi)$ ou $b \in (\pi)$ ce qui signifie que π divise a ou π divise b. Inversement, si π est non nul, non inversible et vérifie le lemme d'Euclide, on a en particulier $(\pi) \neq \{0\}$ et $(\pi) \neq A$ pour les mêmes arguments que précédemment. Si maintenant $a, b \in A$ vérifient $ab \in (\pi)$, alors π divise ab, donc π divise a ou π divise b, soit $a \in (\pi)$ ou $b \in (\pi)$. Ainsi (π) est premier non nul.

2. On suppose de plus A intègre. Supposons par exemple que π vérifie la deuxième condition. Montrons qu'il est irréductible. Par hypothèse, il est non nul et non inversible. Soient $a, b \in A$ tels que $\pi = ab$. En particulier, π divise ab et donc π divise a ou π divise b. Supposons par exemple que π divise a. Alors il existe $u \in A$ tel que $a = u\pi$, et donc $\pi = u\pi b$. Comme A est intègre et $\pi \neq 0$, on obtient $1 = ub$. Par conséquent, $b \in A^*$, donc π est irréductible. ■

Définition. ***(Éléments premiers)***

Un élément $\pi \in A$ est dit *premier* si l'idéal (π) est premier non nul.

Remarques.

1. Tout nombre premier p est un élément premier de $\mathbb{Z}$.
2. De manière évidente, si a et b sont associés, alors a est premier si et seulement si b l'est.
3. En particulier, si π est premier et $u \in A^*$, alors $u\pi$ est premier.
4. **Remarque.** Si A est intègre, tout élément premier est irréductible d'après ce qui précède. Ce n'est plus vrai si A n'est pas intègre. De plus, un élément irréductible n'est pas nécessairement premier : c'est le cas de 2 dans $\mathbb{Z}[i\sqrt{3}]$.

Corollaire

Tout anneau non trivial admet des éléments premiers.

1.3.5 Factorisation dans un anneau

On peut se poser la question suivante : tout élément non nul d'un anneau peut-il se décomposer en produit d'un élément inversible et d'éléments irréductibles ? Si oui, la décomposition est-elle unique à permutation et association près des facteurs ?

On a déjà les réponses négatives suivantes :

- En toute généralité, l'existence d'une telle décomposition est infirmée. On peut exhiber des exemples d'anneaux pour lesquels certains éléments n'ont pas de décomposition.
- Pire, il existe des anneaux qui ne sont pas des corps et qui ne possèdent aucun élément irréductible. C'est le cas de $\mathbb{Z}/6\mathbb{Z}$, ce coquin.
- Dans un anneau où l'existence de la décomposition est assurée, l'unicité ne l'est pas forcément. Il suffit de reprendre l'exemple fondamental de $\mathbb{Z}[i\sqrt{3}]$ développé précédemment et d'observer que $4 = 2^2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$.

Les choses se passent déjà mieux en termes d'unicité lorsqu'on se place dans un anneau intègre et si les éléments intervenant dans la décomposition sont premiers.

Lemme

Soient A un anneau simplifiable. On suppose que l'on a un égalité $up_1...p_r = u'\pi_1...\pi_s$ où r, s sont deux entiers naturels, u, u' inversibles, $p_1, ..., p_r$ premiers et $\pi_1, ..., \pi_s$ irréductibles. Alors $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que $p_i = \pi_{\sigma(i)}$ soient associés pour tout $i \in [\![1, r]\!]$. Puisque associés à des éléments premiers, les $\pi_1, ..., \pi_s$ sont en fait premiers.

▷ On raisonne par récurrence sur r. Traitons d'abord le cas $r = 0$. On a donc $u = u'\pi_1...\pi_s$, soit $u^{-1}u'\pi_1...\pi_s = 1$. Si $s \geqslant 1$, π_1 est inversible ce qui est absurde, car il est irréductible. Ainsi $s = 0$ et la propriété d'association est trivialement vérifiée. Supposons maintenant que ce fait soit vrai pour un entier $r \geqslant 0$ quelconque, et montrons qu'il l'est également au rang $r + 1$. Considérons une égalité du type $up_1...p_{r+1} = u'\pi_1...\pi_s$. Puisque p_1 est premier et que p_1 divise $u'\pi_1...\pi_s$, p_1 divise u' ou p_1 divise l'un des π_j. Mais le premier cas ne peut se produire, car p_1 est premier, donc non inversible, donc il ne peut diviser u', auquel cas il diviserait 1 et serait donc inversible. Ainsi, quitte à changer la numérotation, on peut supposer que p_1 divise π_1. On a donc $\pi_1 = vp_1$ où $v \in A$. Puisque π_1 est irréductible, $p_1 \in A^*$ ou $v \in A^*$. Mais p_1 étant premier, il est non inversible donc $v \in A^*$. ■

2 Principalité

Les développements précédents ont montré que les propriétés arithmétiques de $\mathbb{Z}$ ne sont plus vraies en général dans un anneau quelconque, même intègre. Nous allons maintenant vérifier que dans les anneaux principaux, tout se passe pour le mieux.

2.1 Définition

Définition. ***(Anneau principal)***

Un anneau est dit *principal* s'il est intègre et si tout idéal de A est principal. (En particulier, il est unitaire, commutatif et les idéaux sont automatiquement bilatères.)

Théorème

L'anneau $\mathbb{Z}$ est principal.

▷ Tout l'intérêt de la preuve réside dans ce que les sous-groupes additifs de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ pour un certain $n \in \mathbb{Z}$. Rappelons pourquoi. Soit H un sous-groupe de $\mathbb{Z}$. S'il est trivial, c'est terminé : il est engendré par 0. Sinon, H contient n non nul. Si n est négatif, $-n \in H$ est positif ; quitte à permuter l'un en l'autre, on prend $n \in \mathbb{N}^*$. Ainsi $H \cap \mathbb{N}^*$ est non vide. C'est une partie de $\mathbb{N}$, par propriété fondamentale, elle admet un plus petit élément que nous notons encore n. Montrons que $H = n\mathbb{Z}$. La stabilité additive de H donne que, puisque $n \in H$, $n\mathbb{Z}$ les itérés de n sont aussi dans H. Réciproquement, si $a \in H$, on effectue la division euclidienne de a par n : $a = nq + r$ où $0 \leqslant r < n$. Or si r est non nul, $r = a - nq \in H$ par stabilité additive et $r < n$ ce qui contredit la minimalité de n, donc $r = 0$. Ainsi $a = nq$, donc $a \in n\mathbb{Z}$. Enfin, il est immédiat que les $n\mathbb{Z}$ sont tous des idéaux de $\mathbb{Z}$, et l'on sait aussi que $\mathbb{Z}$ est intègre. ■

Remarque importante. On montre de même, en faisant intervenir le degré, que pour tout corps $\mathbb{K}$, l'anneau des polynômes $\mathbb{K}[X]$ est principal. En effet, si $\mathbb{K}$ est un corps, c'est un anneau intègre donc $\mathbb{K}[X]$ est intègre. Il est pertinent de souligner le rôle de la division euclidienne dans les deux démonstrations précédentes : plus généralement, on verra que tout anneau euclidien est en particulier principal.

Voilà, en guise de récréation, une propriété dont la démonstration a été requise lors des oraux de l'École normale supérieure.

Propriété

Soient a, b dans un anneau commutatif A. Si l'idéal $(a) + (b)$ est principal, il en est de même de l'idéal $(a) \cap (b)$.

▷ On utilise l'intuition donnée par $\mathbb{Z}$ pour nous guider. Soit d un générateur de $(a) + (b)$ (ce qui correspond au pgcd), on pose $a = d\alpha$, $b = d\beta$ et enfin $m = d\alpha\beta$ (ce qui correspond au

ppcm). Montrons par double inclusion que $(a) \cap (b) = (m)$. Soit $x \in (m)$. Il existe $\lambda \in A$ tel que $x = \lambda m = \lambda d\alpha\beta = \lambda a\beta = \lambda\beta a$ et d'autre part $x = \lambda m = \lambda d\alpha\beta = \lambda\alpha d\beta = \lambda\alpha b$, de sorte que $x \in (a) \cap (b)$. Réciproquement, soit $x \in (a) \cap (b)$. On écrit $x = ua = vb$. On sait par ailleurs qu'il existe $\lambda, \mu \in A$ tels que $d = \lambda a + \mu b$. On a alors :

$$x = ua = u\alpha d = u\alpha(\lambda a + \mu b) = \alpha\lambda x + u\mu m = \alpha\lambda vb + u\mu m = m(\lambda\nu + \mu u),$$

d'où la seconde inclusion. ■

2.2 Arithmétique dans les anneaux principaux

La principalité est riche de conséquences arithmétiques.

2.2.1 Conséquences sur la divisibilité

Propriété. ***(Pgcd, ppcm dans un anneau principal)***

Soit A un anneau principal. Soient $a, b \in A$ et $d \in A$ tels que $(a) + (b) = (d)$. Alors d est un pgcd de a et b. Soit $m \in A$ tel que $(a) \cap (b) = (m)$. Alors m est un ppcm de a et b.

▷ D'une part, $a \in (a) + (b)$ donc $a \in (d)$, soit $a = ud$, $u \in A$, donc d divise a. De même d divise b. D'autre part, $d \in (d)$, car A est unitaire. Ainsi $d = au + bv$. Ainsi, si u divise a et b, u divise $au + bv = d$, ce qui montre que d est un *pgcd* de (a, b). La preuve est similaire pour le ppcm. ■

Corollaire. ***(Existences du pgcd et du ppcm)***

Dans un anneau principal, tout couple d'élément admet un pgcd et un ppcm.

▷ Les parties $(a) + (b), (a) \cap (b)$ sont des idéaux de A, ils sont donc principaux. Il suffit donc, d'après la proposition précédente, de considérer au moins un générateur. ■

Propriété

Soit A un anneau principal. Deux éléments sont étrangers si et seulement s'ils sont premiers entre eux.

▷ On sait que deux éléments étrangers sont premiers entre eux. Réciproquement, si 1 est un pgcd de a et b, alors $(a) + (b) = 1A = A$ donc a et b sont étrangers. ■

Théorème. ***(Lemme de Gauss)***

Soient $a, b \in A$ deux éléments premiers entre eux d'un anneau principal. Alors pour tout $c \in A$, si a divise bc, alors a divise c.

▷ Soient $a, b \in A$ principal, premiers entre eux, donc étrangers : $au + bv = 1$. Soit $c \in A$. Alors $acu + bcv = c$. Or a divise bc, donc a divise bcv. De plus a divise acu, donc a divise $acu + bcv = c$, ce qu'il fallait montrer. ■

Théorème. ***(Théorème chinois)***

Soient $a_1, ..., a_n \in A$ principal deux à deux premiers entre eux. Alors les anneaux $A/(a_1...a_n)$ et $A/(a_1) \times ... \times A/(a_n)$ sont isomorphes.

▷ Il suffit d'observer que le morphisme

$$\begin{aligned} f : A &\longrightarrow A/(a_1) \times ... \times A/(a_n) \\ x &\longmapsto ([x]_1, ..., [x]_n) \end{aligned}$$

est surjectif, de noyau $(a_1...a_n)$. ■

2.2.2 Conséquences sur la maximalité des idéaux

Nous allons maintenant nous intéresser de plus près aux éléments irréductibles. Les deux lemmes suivants sont fondamentaux.

Lemme

Soit A un anneau commutatif unitaire et π un élément irréductible. Alors (π) est maximal parmi les idéaux propres principaux de A.

▷ Soit $\pi \in A$ un élément irréductible. Soit $a \in A \setminus A^*$, ce qui revient à prendre le générateur d'un idéal propre de A. On suppose que $(\pi) \subseteq (a)$. Il existe donc b tel que $\pi = ab$ d'après la définition de la divisibilité. Puisque π est irréductible, comme a n'est pas inversible, $b \in A^*$. Mais alors $(\pi) = (a)$, ce qui démontre la maximalité de (π). ■

Lemme

Soit A un anneau principal. Tout irréductible de A engendre un idéal maximal.

▷ Soit $\pi \in A$ un élément irréductible, en supposant A principal. Comme π est non inversible, (π) est propre. En particulier, il existe un idéal maximal $\mathfrak{m}$ contenant (π) d'après le théorème de Krull. Soit $a \in A$ un générateur de $\mathfrak{m}$, qui existe par principalité de A. On a donc $(\pi) \subseteq (a)$, d'où $(\pi) = (a)$ par le point précédent, soit encore $(\pi) = \mathfrak{m}$. Ainsi, $\mathfrak{m}$ est maximal. ■

Propriété. ***(Euclide)***

Dans un anneau principal, un élément est irréductible si et seulement s'il est premier.

▷ L'anneau principal A est intègre, donc tout élément premier est irréductible. Réciproquement, si π est irréductible, (π) est maximal, donc premier, et non nul, car π est non nul. Par définition, π est donc premier. ■

Corollaire

Dans un anneau principal, tout idéal premier non nul est maximal.

▷ Soit $\mathfrak{p}$ un idéal premier non nul. Soit π un générateur de $\mathfrak{p}$. Alors π est irréductible en particulier. D'après le premier lemme, $\mathfrak{p} = (\pi)$ est maximal. ■

Corollaire

Dans un anneau principal, un idéal non nul est premier si et seulement s'il est maximal.

Corollaire

Soit A un anneau principal et π un élément non nul. Les propositions suivantes sont équivalentes :

(i) $A/(\pi)$ est un corps ;

(ii) $A/(\pi)$ est un anneau intègre ;

(iii) π est irréductible.

2.2.3 Conséquences sur la factorisation

Lemme

Soit A un anneau principal. Alors tout élément non nul et non inversible possède un diviseur irréductible.

▷ Soit $a \in A$ un élément non nul et non inversible. Puisque a est non inversible, $(a) \neq A$. L'idéal (a), propre, est donc contenu dans un idéal maximal $\mathfrak{m}$ par le théorème de Krull. En particulier, $\mathfrak{m}$ est un idéal premier, non nul (sinon a serait nul). Posons $\mathfrak{m} = (\pi)$. L'élément π est premier, donc irréductible puisqu'un anneau principal est intègre. Mais alors comme $(a) \subseteq (\pi)$, on obtient π qui divise a, et π est un diviseur irréductible de A. ■

Remarque. En particulier, tout anneau principal qui n'est pas un corps possède au moins un élément irréductible.

Définition. ***(Anneau factoriel)***

Un anneau A est dit *factoriel* s'il est intègre et tout élément non nul $a \in A$ peut s'écrire $a = u\pi_1...\pi_r$, où $\pi_1, ..., \pi_r$ sont irréductibles et $u \in A^*$ et si de plus, cette écriture est unique à permutation et association des facteurs près.

Théorème

Tout anneau principal est factoriel.

▷ Soit A un anneau principal et $a \in A$, $a \neq 0$. Commençons par montrer l'existence d'une décomposition de la forme voulue. Si $a \in A^*$, c'est clair. On suppose donc que A n'est pas un corps, et que a est non nul et non inversible. D'après le lemme précédent, a possède donc au moins un diviseur irréductible $\pi_1 \in A$. On écrit $a = \pi_1 a_1$. Si a_1 est inversible, c'est terminé. Sinon, a_1 divise a, donc $(a) \subseteq (a_1)$ et de plus, si $(a) = (a_1)$, on aurait $a = ua_1$ avec $u \in A^*$, car A est intègre. Mais alors $a = \pi_1 a_1 = ua_1$. Comme $a_1 \neq 0$, car $a \neq 0$, on a, par intégrité, $\pi = u \in A^*$, ce qui est absurde. Ainsi $(a) \subsetneq (a_1)$.

Puisque a_1 est non nul et non inversible, par le lemme, il possède un diviseur irréductible π_2. On écrit $a_1 = \pi_2 a_2$; si a_2 est inversible, on s'arrête. Sinon, comme précédemment, $(a_1) \subsetneq (a_2)$. Supposons que l'élément a_n construit à l'étape n ne soit jamais inversible. Par récurrence, on a alors construit une chaîne infinie d'idéaux $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq ... \subsetneq (a_n) \subsetneq ...$, où $a_n \in A \setminus A^*$ pour tout $n \geqslant 1$.

Posons $a_0 = a$ et soit $\mathfrak{a} = \bigcup_{n\in\mathbb{N}} (a_n)$. On vérifie aisément que $\mathfrak{a}$ est, dans ce cas, un idéal de A. Puisque A est principal, $\mathfrak{a} = (x)$. En particulier, il existe un certain entier naturel j tel que $x \in (a_j)$. On a alors $(x) \subseteq (a_j) \subseteq \mathfrak{a} = (x)$, d'où $(x) = (a_j)$. Mais ceci est contradictoire, car $(x) = (a_j) \subsetneq (a_{j+1}) \subseteq x$, et donc $(x) \subsetneq (x)$.

Ainsi, il existe $n \geqslant 1$ tel que $a_{n+1} \in A^*$. En posant $u = a_{n+1}$, on obtient $a = u\pi_1...\pi_n$, ce qui est la décomposition cherchée.

L'unicité de la décomposition découle du lemme correspondant sur les anneaux simplifiables, puisqu'en vertu du lemme de la section précédente, tout élément irréductible est ici premier. ■

Note générale

On appelle *anneau noethérien* un anneau commutatif dont tout idéal de A peut être engendré par un nombre fini d'éléments, ou, ce dont on peut montrer que cela revient au même, si toute suite croissante d'idéaux est stationnaire. Alors, on montre que tout anneau principal est noethérien, et que tout anneau noethérien est factoriel.

Pour conclure, on peut définir le concept suivant permettant de formaliser la réelle unicité de la décomposition.

Définition. ***(Système complet de représentants irréductibles)***

Soit A un anneau. Un *système complet de représentants irréductibles* est un sous-ensemble P de A composé d'irréductibles tel que tout irréductible de A soit associé à exactement un élément de P.

Proposition

Tout anneau possède au moins un système complet de représentants irréductibles.

▷ Il suffit de prendre un système de représentant de la relation d'équivalence d'association, qui existe toujours d'après l'axiome du choix. ■

Reformulation

Soit A un anneau principal, P un système complet de représentants irréductibles. Tout élément non nul de A s'écrit sous la forme $a = u \prod_{\pi \in P} \pi^{n_\pi}$ où u est inversible et les (n_π) sont des entiers naturels presque tous nuls. Cette décomposition est unique au sens des u et (n_π).

2.3 Principalité des anneaux euclidiens

On termine cet exposé de la notion d'anneau principal sur un théorème permettant de vérifier aisément qu'un anneau est principal. En effet, dans les cas complexes, il est souvent plus facile d'exhiber une division euclidienne sur un anneau que de vérifier que tous les idéaux de l'anneau sont engendrés chacun par un seul élément.

Définition. ***(Anneau euclidien)***

Un anneau A est dit *euclidien* s'il est intègre et s'il existe une application appelée *stathme euclidien* $\delta : A \setminus \{0\} \longrightarrow \mathbb{N}$ telle que pour tout $a \in A$ et pour tout $b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que $a = bq + r$, et $r = 0$ ou $\delta(r) < \delta(b)$.

Remarque. On ne demande pas l'unicité de q ni de r.

Théorème

Tout anneau euclidien est principal.

▷ Supposons (A, δ) euclidien. Alors A est intègre par définition. Soit I un idéal de A. Si I est nul, il n'y a rien à faire. On peut donc supposer qu'il ne l'est pas. On considère l'ensemble $E = \{\delta(a), a \in I \setminus \{0\}\}$. L'ensemble E est une partie non vide de $\mathbb{N}$, par propriété fondamentale, elle admet donc un plus petit élément que nous notons $a_0 \in I \setminus \{0\}$. On va donc montrer que $I = (a_0)$. Puisque I est un idéal de A contenant a_0, on a $(a_0) \subseteq I$. Réciproquement, soit $a \in I$. On écrit $a = qa_0 + r$ avec $r = 0$ ou $\delta(r) < \delta(a_0)$. Puisque a et a_0 sont des éléments de I, $r = a - qa_0 \in I$

puisqu'un idéal est en particulier un sous-groupe. Si r était non ul, on aurait alors $r \in I \setminus \{0\}$ et $\delta(r) < \delta(a_0)$, ce qui contredirait le choix de a_0. Par conséquent, $r = 0$ et $a = qa_0 \in I$. Par double inclusion, $I = (a_0)$, ce qui conclut la preuve. ■

3 Utilisation de la factorialité de $\mathbb{Z}$ pour la résolution d'équations diophantiennes

La première propriété énonce de façon complète les solutions de l'équation des triplets pythagoriciens.

Proposition

Si $x^2 + y^2 = z^2$, x, y, z des entiers supérieurs à 1, il existe un entier d et des entiers premiers entre eux u, v tels qu'à permutation près de x et y, on ait $x = d(u^2 - v^2)$ et $y = 2duv$. Réciproquement, en posant $z = d(u^2 + v^2)$, ces entiers donnent des solutions de l'équation de Pythagore.

En utilisant ce résultat, on obtient le lemme suivant :

Lemme

L'équation $x^4 + y^4 = z^2$ n'a pas de solutions dans $\mathbb{N}^{*3}$.

d'où l'on déduit immédiatement le cas particulier du théorème de Fermat dans le cas $n = 4$:

Théorème

L'équation $x^4 + y^4 = z^4$ n'a pas de solutions dans $\mathbb{N}^{*3}$.

4 Conclusion

Un dessin vaut mieux qu'un long discours :

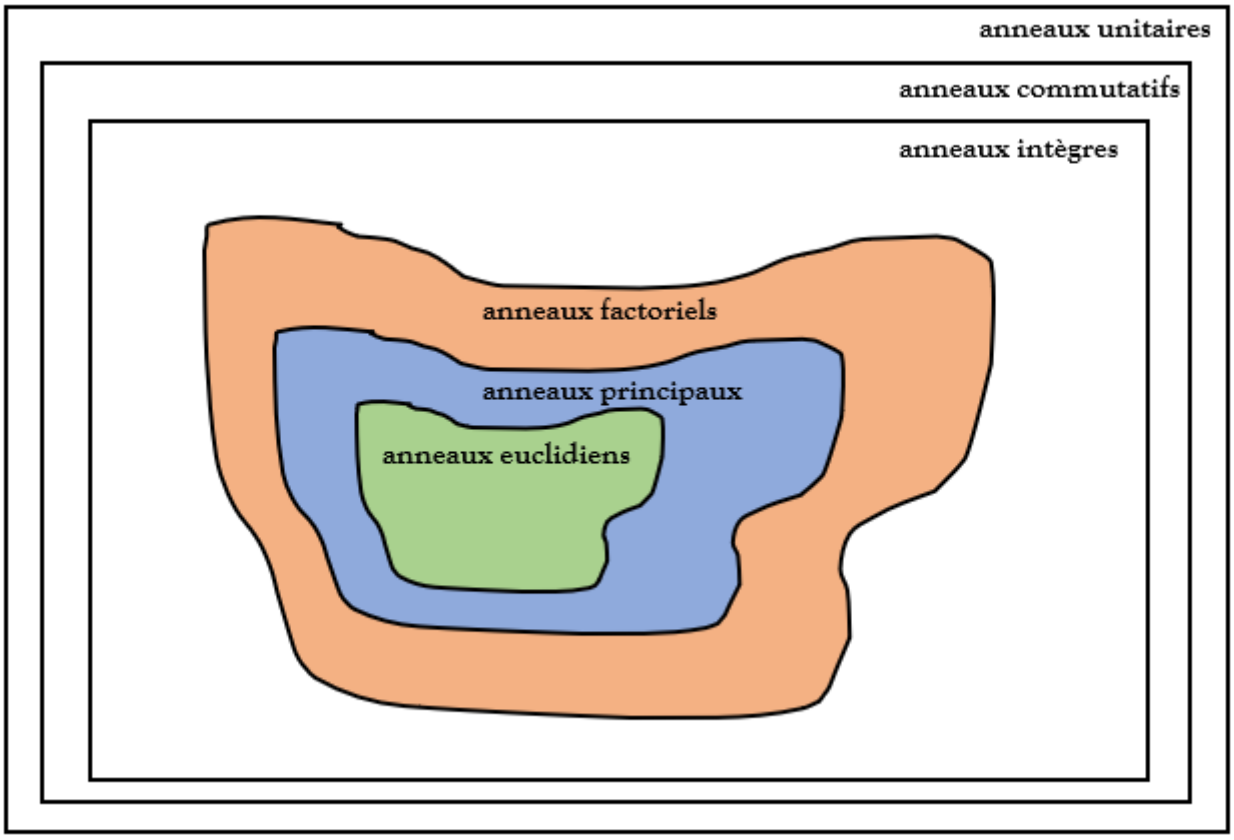

FIGURE 1. — *Structures particulières d'anneaux.* Les anneaux euclidiens forment la classe d'anneaux la plus restrictive que nous avons étudiée dans ce document. Parmi tous, les anneaux intègres constituent la classe ne possédant aucune propriété intéressante du point de vue de l'arithmétique. Travail personnel.

Table des matières

A Bibliographie

Références

[1] *Algèbre : le grand combat. Cours et exercices*, Grégory Berhuy, 2018, Calvage et Mounet, 2e éd.

[2] *Mathématiques. Tout-en-un pour la Licence*, sous la direction de Jean-Pierre Ramis, André Warusfel, 2006, Dunod, 2e éd., vol. 2

[3] *Les maths en tête : Algèbre, probabilités*, Xavier Gourdon, 2021, Ellipses, 3e éd., vol. 2

[4] *Oraux x-ens mathématiques*, Serge Nicolas, Serge Francinou, Hervé Gianella, Cassini, vol. 1