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.

En particulier, $a_1, \dots, a_n$ sont dits premiers entre eux si 1 en est un pgcd.

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 $a_1, \dots, a_n \in A \setminus \{0\}$ 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. □

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 $aA = \{ax \mid x \in A\}$ 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 un élément de A. Typiquement, chez Kummer, A est un sous-anneau d'un anneau B, et pour $b \in B$ (le « nombre idéal ») et il considère l'idéal $I = bB \cap A$ de A.

Indiquons quelques constuctions générales d'idéaux :

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.

(a) (Sommes) Si $(I_j)_{j\in J}$ est une famille d'idéaux de A (avec J finie ou non), on désigne par $\sum_j I_j$ l'ensemble des sommes finies d'éléments de $\bigcup_j I_j$. C'est le plus petit idéal de A contenant les I_j. Pour $a_1, \dots, a_n \in A$, on pose aussi

$$(a_1, \dots, a_n) = a_1A + a_2A + \cdots + a_nA = \{\sum_{i=1}^{n} a_i x_i \mid x_i \in A \ \forall i\}.$$

Un idéal de A de cette forme est dit *de type fini*, ou *finiment engendré*.

(b) (Intersections) De même, si $(I_j)_{j\in J}$ est une famille d'idéaux de A, alors $\cap_j I_j$ est un idéal de A : c'est le plus grand idéal inclus dans tous les I_j.

Les notions de somme et d'intersection sont donc les analogues dans le langage des idéaux des notions respectives de pgcd et ppcm pour les éléments. Elles existent toujours : c'est une première indication du fait que les idéaux se comportent mieux que les éléments.

(c) (Comportement vis-à-vis des morphismes) Soit $f : A \to B$ un morphisme d'anneaux. Alors $\ker f := \{a \in A \mid f(a) = 0\}$ est un idéal de A. Plus généralement, si I est un idéal de B alors $f^{-1}(I)$ est un idéal de A. Enfin, si f est surjective, et si I est un idéal de A, alors $f(I)$ est un idéal de B. À bien des égards, *les idéaux sont aux anneaux ce que les sous-groupes distingués sont aux groupes*. Nous renvoyons au Complément 9 pour une discussion de la notion importante d'*anneau quotient*.

Définition 4.3. *Un anneau est dit* noethérien *si ses idéaux sont de type fini.*

Les Propositions 4.4 et 4.5 suivantes ont été mentionnées sans démonstration en classe. Les anneaux noethériens seront étudiés plus en détail en cours d'Algèbre 2.

Proposition 4.4. *Soit A un anneau commutatif. Il y a équivalence entre :*

(i) A est noethérien,

(ii) toute suite croissante *$(I_m)_{m\geqslant 1}$ d'idéaux de A, c'est-à-dire avec $I_m \subset I_{m+1}$ pour tout $m \geqslant 1$, est constante à partir d'un certain rang.*

(iii) toute famille non vide d'idéaux de A admet un élément maximal pour l'inclusion.

Démonstration — Pour (i) $\implies$ (ii), on constate que $I = \bigcup_{m\geqslant 1} I_m$ est un idéal de A, car $(I_m)_{m\geqslant 1}$ est croissante. Il est donc de la forme $(a_1, \dots, a_n)$ pour certains éléments $a_i \in A$. Si N est assez grand de sorte que $a_i \in I_N$ pour $i = 1, \dots, n$, on constate $I_m \subset I \subset I_N$ pour tout $m \geqslant 1$, d'où l'on tire $I_m = I_N$ si $m \geqslant N$.

Le (ii) implique (iii) dans tout ensemble ordonné : s'il n'y a pas d'élément maximal, on fabrique par induction une suite strictement croissante d'éléments.

Montrons enfin que (iii) implique (i). Soit I un idéal de A. Soit $\mathscr{F}$ l'ensemble des idéaux de type fini de A inclus dans I, ordonné par l'inclusion. Il contient $\{0\} = 0A$ donc est non vide. Par le (iii), il admet un élément maximal, disons $J \subset I$. Si $J \neq I$, il existe $x \in I\backslash J$, et on a donc $J \subsetneq J + xA \subset I$, une contradiction car $J + xA$ est de type fini. Cela montre que $I = J$ est de type fini. □

PROPOSITION 4.5. *Si A est intègre noethérien alors A vérifie* (PF).

DÉMONSTRATION — Soit $S \subset A \setminus \{0\}$ l'ensemble des éléments qui sont produits d'unités et d'irréductibles. Si $a \notin S$, alors a n'est pas irréductible, et donc de la forme bc avec b et c non unités. Comme S est stable par produits, soit b soit c n'est pas dans S. Si $S \neq A \setminus \{0\}$, on construit donc récursivement une suite d'éléments non nuls $a_m \in A \setminus S$ pour $m \geqslant 1$ avec a_{m+1} divise a_m et a_m non associé à a_{m+1}. Ainsi, $I_m = (a_m)$ est une suite strictement croissante d'idéaux de A, ce qui est absurde par noethérianité . □

5. Anneaux principaux

DÉFINITION 5.1. *Un anneau principal est un anneau intègre dont tous les idéaux sont principaux.*

Un anneau principal est trivialement noethérien. Dans un anneau principal, on a des relations de Bezout :

PROPOSITION 5.2. (Relations de Bézout) *Soient A un anneau principal et $a, b \in A$. Alors a et b admettent un pgcd d dans A, et il existe $u, v \in A$ tels que $au + bv = d$.*

DÉMONSTRATION — L'idéal $aA + bA$ est principal, donc de la forme dA pour un certain $d \in A$. On a $a, b \in dA$, donc d est un diviseur de a et de b. On a aussi $d \in aA + bA$, donc il existe $u, v \in A$ avec $d = au + bv$, et tout diviseur de a et b divise donc d : c'est un pgcd. □

Le résultat principal de cette section est alors le suivant.

THÉORÈME 5.3. *Un anneau principal est factoriel.*

DÉMONSTRATION — Un anneau principal est clairement noethérien, donc satisfait (PF) par la Proposition 4.5. D'après la Proposition 3.3, il suffit donc de montrer que tout irréductible π de l'anneau principal A, alors π est premier.

Supposons donc que π divise ab avec $a, b \in A$. Soit d un pgcd de π et a. C'est un diviseur de l'irréductible π, donc on a soit $d \sim 1$, soit $d \sim \pi$. Dans le second cas on a $\pi \sim d$ divise a. Dans le premier, on a $1 = \pi u + av$ avec $u, v \in A$, et donc $b = \pi bu + abv$, puis π divise b. □

6. Anneaux euclidiens et exemples

DÉFINITION 6.1. *Un anneau commutatif A est dit euclidien s'il possède une fonction $\varphi : A\backslash\{0\} \to \mathbb{N}$ telle que $\forall a, b \in A\backslash\{0\}$, il existe q et $r \in A$ tels que $a = bq + r$ avec :*

(i) soit $r = 0$,

(ii) soit $r \neq 0$ et $\varphi(r) < \varphi(b)$.

On appelle *stathme euclidien* une telle fonction (du grec ancien $\sigma\tau\alpha\theta\mu\nu$ signifiant « *fil à plomb, règle, mesure* », la terminologie semble due à F. Dress [2]). On parle aussi communément de *fonction euclidienne* ou d'*algorithme euclidien.*

EXEMPLE 6.2. (i) *L'anneau* $\mathbb{Z}$ *est euclidien pour* $\varphi(n) = |n|$. De même, l'anneau $\mathbb{Z}/N\mathbb{Z}$ est euclidien pour $\varphi(\overline{n}) = n$ pour $n \in \{0, \dots, N-1\}$.

(ii) *Pour* k *un corps, l'anneau* $k[X]$ *est euclidien pour* deg.

(iii) Pour k commutatif général, $k[X]$ n'est pas nécessairement euclidien. Néanmoins pour tout $A, B \in k[X]$ avec B *unitaire*, il existe $P, Q \in k[X]$ tels que $A = BQ + R$, avec soit $R = 0$, soit $R \neq 0$ et $\deg R < \deg B$.

PROPOSITION 6.3. *Pour* $d = -2, -1, 2$*, l'anneau* $\mathbb{Z}[\sqrt{d}]$ *est euclidien pour* $|\mathrm{N}|$.

DÉMONSTRATION — Observons qu'il suffit de montrer que pour tout $t \in \mathbb{Q}[\sqrt{d}]$, il existe $q \in \mathbb{Z}[\sqrt{d}]$ avec $|\mathrm{N}(t-q)| < 1$. En effet, si on a $a, b \in \mathbb{Z}[\sqrt{d}]$ avec $a, b \neq 0$, appliquant ceci à $t = a/b \in \mathbb{Q}[\sqrt{d}]$ il existe $q \in \mathbb{Z}[\sqrt{d}]$ avec $|\mathrm{N}(a/b - q)| < 1$. Par multiplicativité de la norme, on a $|\mathrm{N}(a - bq)| < |\mathrm{N}(b)|$ puis $r := a - qb$ convient.

Pour montrer l'observation on écrit $t = x + y\sqrt{d}$ avec $x, y \in \mathbb{Q}$. Il existe $u, v \in \mathbb{Z}$ avec $|u - x| \leqslant 1/2$ et $|v - y| \leqslant 1/2$. Posons $q = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. On a bien $|\mathrm{N}(t-q)| \leqslant (x-u)^2 + |d|(y-v)^2 \leqslant \frac{1+|d|}{4} < 1$ pour $|d| < 3$. □

PROPOSITION 6.4. *Un anneau intègre euclidien est principal.*

DÉMONSTRATION — L'idéal nul étant principal, il suffit de voir que tout idéal non nul I de A est principal. Soit φ un stathme euclidien sur A, la partie $\varphi(I\backslash\{0\}) \subset \mathbb{N}$ est non vide, on peut donc trouver un élément $b \in I\backslash\{0\}$ pour lequel $\varphi(b)$ est minimal. Bien entendu, on a $bA \subset I$. Vérifions l'inclusion réciproque. Soit $a \in I$. Il existe $q, r \in A$ tels que $a = bq + r$, avec de plus $\varphi(r) < \varphi(b)$ si r est non nul. Mais $r = a - bq \in I$ car I est un idéal, donc on a $r = 0$ par minimalité de $\varphi(b)$. On a donc $a = bq$ puis $I \subset bA$, et $I = bA$. □

COROLLAIRE 6.5. *Les anneaux* $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$*, ainsi que* $k[X]$ *quand* k *est un corps, sont principaux, et donc factoriels.*

REMARQUE 6.6. *Toujours si* k *est un corps, l'anneau* $k[X, Y]$ *n'est pas principal. Par exemple, l'idéal* (X, Y) *n'est pas principal (pourquoi ?). En revanche, on peut montrer que* $k[X_1, \dots, X_n]$ *est factoriel pour tout* $n \geqslant 1$ *(voir l'Exercice 7.20). En particulier, il existe des anneaux factoriels non principaux.*

Terminons par des remarques culturelles sur la famille d'anneaux $\mathbb{Z}[\sqrt{d}]$.

REMARQUE 6.7. (i) On peut montrer que pour les anneaux $\mathbb{Z}[\sqrt{d}]$, *principal équivaut à factoriel* : voir l'Exercice 7.30.

2. F. Dress, Stathmes euclidiens et séries formelles, Acta Arithmetica (1971).

(ii) Il n'est pas difficile de montrer que l'anneau $\mathbb{Z}[\sqrt{d}]$ n'est jamais principal pour $d < -2$: voir l'Exercice 7.5. En revanche, c'est un problème ouvert de déterminer les entiers $d > 0$ tels que $\mathbb{Z}[\sqrt{d}]$ est principal. Les premiers sont $d = 2, 3, 6, 7, 11, 14, 19, 22, 23, 31$: voir cette suite. On ne sait même pas s'il y en a un nombre fini !

(iii) On conjecture qu'il y a une infinité d'entiers $d > 0$ tels que $\mathbb{Z}[\sqrt{d}]$ est euclidien. On sait que $\mathbb{Z}[\sqrt{d}]$ est euclidien pour $|\mathrm{N}|$ si, et seulement si, $d = -2, -1, 2, 3, 6, 7, 11, 19$ (Chatland-Davenport, Inkeri). Il a été démontré seulement en 2004 par Harper que $\mathbb{Z}[\sqrt{14}]$ est euclidien (mais pas pour $|\mathrm{N}|$, donc).

7. L'anneau $\mathbb{Z}[i]$ et sommes de deux carrés

On a vu que l'anneau $\mathbb{Z}[i]$ est euclidien, donc principal, donc factoriel. Ainsi, tout entier de Gauss non nul est produit de manière unique d'une des 4 unités $\pm 1, \pm i$ et d'irréductibles de $\mathbb{Z}[i]$ (disons appartenant à un système de représentants fixé). Pour utiliser ce résultat, il est important de savoir décrire ces irréductibles :

THÉORÈME 7.1. *Tout irréductible de $\mathbb{Z}[i]$ divise un et un seul nombre premier $p \in \mathbb{Z}$ usuel. De plus, pour un tel p on est dans un et un seul des cas suivants :*

(i) $p = 2$, et on a $2 = -i(1+i)^2$ avec $1+i$ irréductible (de norme 2),

(ii) $p \equiv 3 \bmod 4$, et p est irréductible dans $\mathbb{Z}[i]$ (de norme p^2),

(iii) $p \equiv 1 \bmod 4$, et on a $p = \pi\overline{\pi}$ avec π et $\overline{\pi}$ des irréductibles de $\mathbb{Z}[i]$ non associés (de norme p).

DÉMONSTRATION — Soit π un irréductible de $\mathbb{Z}[i]$. Alors $n := \mathrm{N}(\pi) = \pi\overline{\pi}$ est un entier $n > 1$. Comme π est premier, car $\mathbb{Z}[i]$ est principal, il divise donc dans $\mathbb{Z}[i]$ l'un des facteurs premiers de n dans $\mathbb{Z}$. Soit p un tel facteur. On a $p = \pi\eta$ avec $\eta \in \mathbb{Z}[i]$. On en déduit $p^2 = \mathrm{N}(\pi)\mathrm{N}(\eta)$, puis $\mathrm{N}(\pi) = p$ ou p^2. Cela montre que p est uniquement déterminé par π et conclut la première assertion. Il reste à décomposer en irréductibles dans $\mathbb{Z}[i]$ chaque premier p usuel (!).

L'assertion sur $p = 2$ est claire. Supposons $p \equiv 3 \bmod 4$. Si p n'est pas irréductible, on peut écrire $p = \alpha\beta$ avec α, β dans $\mathbb{Z}[i]$ de normes > 1. Comme on a $\mathrm{N}(p) = p^2 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, on a donc $\mathrm{N}(\alpha) = p$. Écrivant $\alpha = a + bi$ avec $a, b \in \mathbb{Z}$ on a alors $p = a^2 + b^2$. Comme p est impair, alors a et b n'ont pas même parité, et donc on a $p \equiv 1 \bmod 4$: contradiction.

Supposons enfin $p \equiv 1 \bmod 4$. Montrons que p n'est pas irréductible. En effet, on sait que -1 est un carré modulo p (Euler). Il existe donc $n \in \mathbb{Z}$ tel que p divise n^2+1. On a la décomposition $n^2+1 = (n+i)(n-i)$ dans $\mathbb{Z}[i]$. Si p était irréductible dans $\mathbb{Z}[i]$, il serait premier (car $\mathbb{Z}[i]$ factoriel), et on aurait donc $p \mid n+i$ ou $p \mid n-i$ dans $\mathbb{Z}[i]$. C'est absurde car $p\mathbb{Z}[i]$ est l'ensemble des $a + bi$ avec $a \in p\mathbb{Z}$ et $b \in p\mathbb{Z}$, et $n \pm i$ n'a pas cette propriété. On en déduit $p = \alpha\beta$ avec α, β non inversibles, puis $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = p$ comme plus haut. Posons $\pi = \alpha = a + bi$. On a montré $p = \mathrm{N}(\pi) = a^2 + b^2$, et donc redémontré que p est somme de deux carrés. En outre π est irréductible car de norme première, et $p = \pi\overline{\pi}$ est donc sa décomposition en irréductibles. Il ne reste qu'à voir que π et $\overline{\pi}$ sont non associés. Mais comme on a $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, les associés de $\pi = a + bi$ sont $a + bi$, $-a - bi$, $-b + ai$ et $b - ai$.

Cette liste contient $\overline{\pi} = a - bi$ si, et seulement si, $b = 0$, $a = 0$ ou $a = \pm b$, et donc $p = a^2$, b^2 ou $p = 2a^2$: aucune de ces solutions n'est possible (on a $p > 2$). □

Le point (iii) du Théorème ci-dessus redémontre en particulier que tout premier $p \equiv 1 \bmod 4$ est somme de 2 carrés (Fermat) : c'est la troisième démonstration que nous en donnons, et sans doute la plus conceptuelle ! De plus, la factorialité de $\mathbb{Z}[i]$ permet aussi de comprendre de manière limpide l'unicité d'une telle écriture, un résultat dû à Gauss (voir le Lemme 1.7 Chap. 3) :

PROPOSITION 7.2. *Tout nombre premier $p \equiv 1 \bmod 4$ s'écrit de manière unique sous la forme $p = a^2 + b^2$ avec $a, b \in \mathbb{N}$.*

DÉMONSTRATION — Soit p premier $\equiv 1 \bmod 4$. On a vu que la décomposition en irréductibles de p dans $\mathbb{Z}[i]$ est $p = \pi\overline{\pi}$, avec π et $\overline{\pi}$ des irréductibles (non associés). En particulier, posant $\pi = a + bi$, on a $p = a^2 + b^2$.

Supposons maintenant que l'on a $x, y \in \mathbb{Z}$ avec $x^2 + y^2 = p$. L'élément $z = x + ix$ vérifie donc $\mathrm{N}(z) = p = z\overline{z}$. C'est donc un facteur irréductible (car de norme première) de p dans $\mathbb{Z}[i]$. Par factorialité de $\mathbb{Z}[i]$, les seules possibilités sont donc $z \sim \pi$ ou $z \sim \overline{\pi}$. Mais on a $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, de sorte que les 4 associés de π sont $a + bi$, $-a - bi$, $-b + ai$ et $b - ai$, et ceux de $\overline{\pi}$ sont $a - bi$, $-a + bi$, $-b - ai$, et $b + ai$. Au final, on a bien $(x, y) = (\pm a, \pm b)$ ou $(\pm b, \pm a)$. □

L'arithmétique de $\mathbb{Z}[i]$ permet plus généralement de déterminer, pour tout entier $n \geqslant 0$, le nombre de couples $(a, b) \in \mathbb{Z}^2$ avec $n = a^2 + b^2$: voir l'Exercice 7.4.

8. Une équation diophantienne

Donnons une application typique de la factorialité des anneaux de la forme $\mathbb{Z}[\sqrt{d}]$ à l'étude des équations diophantiennes. La proposition suivante avait été formulée par Fermat. On prétend qu'il l'avait lancé en défi aux mathématiciens anglais de son époque (le milieu du 17^{eme} siècle).

PROPOSITION 8.1. *Les seules solutions $x, y \in \mathbb{Z}$ de l'équation $y^2 = x^3 - 2$ sont les solutions évidentes $(x, y) = (3, \pm 5)$.*

DÉMONSTRATION — Soient $x, y \in \mathbb{Z}$ tels que $y^2 = x^3 - 2$. Comme 2 n'est pas un cube dans $\mathbb{Z}/4\mathbb{Z}$, on constate que y est impair. Considérons la factorisation

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$$

dans $\mathbb{Z}[\sqrt{-2}]$. On a vu que ce dernier est euclidien, donc principal et factoriel. Vérifions que $y + \sqrt{-2}$ et $y - \sqrt{-2}$ sont premiers entre eux dans $\mathbb{Z}[\sqrt{-2}]$. Il suffit de voir qu'il n'y a pas d'irréductible π divisant $y + \sqrt{-2}$ et $y - \sqrt{-2}$. Mais un tel π diviserait $2\sqrt{-2} = -\sqrt{-2}^3$, et donc $\sqrt{-2}$ (car π est également premier), et donc y. Mais alors $\mathrm{N}(\sqrt{-2}) = 2$ diviserait $\mathrm{N}(y) = y^2$ dans $\mathbb{Z}$: absurde car y est impair.

Si dans un anneau factoriel A, on a une relation $a^n = bc$ avec b et c premiers entre eux, et n un entier $\geqslant 1$, on constate en décomposant b et c en irréductibles qu'il existe $d \in A$ et $u \in A^\times$ tels que $b = d^n u$. Comme on a montré $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$,

on en déduit l'existence de $z \in \mathbb{Z}[\sqrt{-2}]$ tel que $y + \sqrt{-2} = \pm z^3 = (\pm z)^3$. Posons $\pm z = u + v\sqrt{-2}$ avec $u, v \in \mathbb{Z}$. On a donc

$$y + \sqrt{-2} = (u + v\sqrt{-2})^3 = u^3 - 6uv^2 + (3u^2v - 2v^3)\sqrt{-2}.$$

En prenant la coordonnée en $\sqrt{-2}$, il vient $1 = v(3u^2 - 2v^2)$, d'où l'on tire $v = \pm 1$ puis $3u^2 = v + 2$ et donc $v = 1$ et $u = \pm 1$. On a donc $y = u^3 - 6uv^2 = \pm 5$, puis $x^3 = 27$, et donc nécessairement $x = 3$, ce qui conclut ! □

Cette méthode admet de multiples applications. La plus célèbre est certainement la stratégie qu'elle fournit pour étudier l'équation de Fermat $x^n + y^n = z^n$, qui s'écrit aussi $x^n = \prod_{i=0}^{n-1}(z - \zeta^i y)$ où $\zeta = e^{\frac{2i\pi}{n}}$. Plusieurs mathématiciens ont crû démontrer ainsi, avec du travail, le *grand théorème de Fermat*. Malheureusement, le sous-anneau $\mathbb{Z}[\zeta] = \sum_{k=0}^{n-1} \mathbb{Z}\zeta^k \subset \mathbb{C}$ est rarement factoriel (le premier cas problématique étant $n = 23$), et il faut se plonger dans la théorie de Kummer pour comprendre comment remédier partiellement à ce problème. Nous renvoyons à tout cours de théorie algébrique des nombres, par exemple à celui de l'auteur, pour une étude de ces questions.