## 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 $\mathbf{Z}[i]$.

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 $c$.*

*Démonstration.* Le fait que tout anneau intègre vérifie la propriété « premier entraîne irréductible » a été démontrée au chapitre 2 (théorème 67).

On trouvera ci-dessous la démonstrations des autres assertions. *Il est vivement conseillé de commencer par chercher ces démonstrations soi-même à titre d'exercice.*

Démontrons le lemme d'Euclide faible. Soit donc soit $a, b, c \in A$ tel que si $aA$ est un idéal premier non nul et $a$ divise $bc$. Montrons que $a$ divise $b$ ou $a$ divise $c$. Comme $a$ divise $bc$, $bc$ est un élément de $aA$. Comme $aA$ est un idéal premier, on a donc $b \in aA$ ou $c \in aA$. Ceci signifie exactement que $a$ divise $b$ ou $a$ divise $c$.

Démontrons le théorème de Bézout faible. Soit $a, b \in A$ tel que $aA + bA = A$. Montrons que $a$ et $b$ sont premiers entre eux. Soit $d$ un diviseur commun de $a$ et $b$. Comme $aA+bA = A$, on a $1_A \in aA + bA$. Il existe donc $(u, v) \in A^2$ tels que $au + bv = 1_A$. Comme $d$ divise $a$ et $b$, la relation précédente montre que $d$ divise $1_A$. Donc $d$ est inversible, et $a$ et $b$ sont premiers entre eux.

Démontrons le lemme de Gauss faible. Soit $a, b, c \in A$ tel que $a$ divise $bc$ et $aA + bA = A$.Montrons que $a$ divise $c$. Comme précédemment, il existe donc $(u, v) \in A^2$ tels que $au + bv = 1_A$. En multipliant cette relation par $c$, on obtient $acu + bcv = c$. Or $a$ divise $bc$ (donc $bcv$) par hypothèse et $a$ divise évidemment $acu$, donc $a$ divise $c$. □

*Remarque.* Ces versions affaiblies de certaines propriétés de la définition 1 sont donc vraies pour un anneau intègre quelconque mais elles sont dans la pratique *infiniment* moins utiles que les versions fortes correspondantes. Il est conseillé de prendre le temps de relire la définition 1 et de comparer avec l'énoncé de la proposition pour comprendre en quel sens on parle de versions affaiblies.

*Remarque.* On peut aussi considérer une version affaiblie du théorème de factorisation unique : le même énoncé mais sans la propriété d'unicité. Cependant, contrairement aux propriétés « faibles » considérées dans la proposition 2, cette propriété d'existence d'une

décomposition en produits d'irréductibles n'est pas vérifiée par tous les anneaux intègres. Les anneaux intègres qui la vérifient sont appelés parfois *anneaux atomiques*[15], et en anglais également *factorization domain*. Là encore, insistons sur le fait que dans la pratique la simple existence d'une décomposition en irréductibles est infiniment moins utile que la version forte correspondante, c'est-à-dire la version avec unicité.

On peut montrer que l'anneau $\mathbf{Z}[i\sqrt{3}]$ est atomique (on a déjà remarqué qu'il ne vérifiait pas la propriété d'unicité de la décomposition), ainsi que les anneaux $\mathbf{Z}[\zeta_p]$ considéré dans la première section du chapitre. En fait on peut montrer plus généralement que tout anneau intègre *noetherien* est atomique. Les anneaux noetheriens forment une classe extrêmement vaste et utile d'anneaux (qui n'est pas au programme de ce module). Un anneau est noetherien si tout idéal est engendré par un nombre fini d'éléments. Quasiment tous les exemples explicites d'anneaux considérés dans ce cours sont noetheriens. Les anneaux atomiques sont donc « très nombreux dans la pratique ».

On peut montrer que l'anneau des fonctions holomorphes entières est un anneau intègre non atomique.

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.*

*Démonstration.* Pour la première assertion, compte tenu de la proposition 2, il s'agit en fait de montrer que le lemme d'Euclide est équivalent à la propriété « irréductible entraîne premier ». Mais on constatera facilement que pour un élément irréductible $a$, le lemme d'Euclide exprime exactement le fait que l'idéal $aA$ est premier (noter que si $a$ est irréductible, l'idéal $aA$ est nécessairement propre).

Supposons que $A$ vérifie le lemme de Gauss. Soit $a, b, c \in A$ tels que $a$ est irréductible et divise $bc$. Supposons que $a$ ne divise pas $b$. D'après la proposition 66 du chapitre 2, $a$ et $b$ sont premiers entre eux. Comme $A$ vérifie le lemme de Gauss, $a$ divise $c$. Ainsi $A$ vérifie bien le lemme d'Euclide.

Si $A$ vérifie le théorème de Bézout, comme $A$ vérifie de toute façon le lemme de Gauss faible (*cf.* proposition 2), $A$ vérifie bien le lemme de Gauss. □

15. Rappelons qu'étymologiquement, un atome est quelque chose qu'on ne peut pas couper en éléments plus petits ; dans ce contexte, les atomes sont les éléments irréductibles

*Remarque* 22. La terminologie employée ici, quoiqu'à ma connaissance assez standard dans la littérature francophone, n'est pas universellement utilisée. Ce que nous appelons ici *lemme de Gauss* est parfois appelé *lemme d'Euclide généralisé* voire...*lemme d'Euclide* (et dans ce dernier cas ce que nous appelons ici lemme d'Euclide est en général évoqué sous la forme « irréductible=premier »).

### 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

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

*Remarque.* Une application $\nu$ comme dans l'énoncé est appelée *stathme euclidien* ou parfois *préstathme euclidien* (dans ce dernier cas, un stathme est un préstathme vérifiant une propriété supplémentaire, nous n'aurons pas besoin de cette nuance au niveau de ce cours).

Si $A$ est euclidien, muni d'un stathme $\nu$, et $(a, b) \in A \times (A \setminus \{0\})$, une écriture $a = bq + r$ et avec $(q, r) \in A^2$ et soit $r = 0$, soit $\nu(r) < \nu(b)$ est appelée *division euclidienne de $a$ par $b$* (par rapport au stathme euclidien $\nu$)

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.*

*Remarque.* Comme il existe des anneaux factoriels non principaux (nous en verrons des exemples ci-dessous), ceci montre en particulier qu'il existe des anneaux intègres qui vérifient le lemme de Gauss mais pas le théorème de Bezout.

Tous les résultats énoncés précédemment seront démontrés ci-après, sauf l'existence d'anneaux principaux non euclidiens, un peu délicate [16].

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.

*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 $\nu_p$ (*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

16. 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.

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 » :*

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

*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).*

*Démonstration.* La démonstration, qui donnera également un moyen effectif d'effectuer les divisions euclidiennes dans $\mathbf{Z}[i]$ est basée sur l'observation géométrique élémentaire suivante : pour tout élement $x$ de $\mathbf{R}^2$ il existe un élément $y$ de $\mathbf{Z}^2$ telle que la distance de $x$ à $y$ est strictement inférieur à 1. Faire un dessin et se ramener à l'énoncé suivant : tout point d'un carré de côté 1 est à distance strictement inférieure à 1 de l'un des sommets du carré. En fait l'inégalité triangulaire montre que pour tout point d'un tel carré, il existe un sommet du carré à distance de ce point inférieure à $\frac{\sqrt{2}}{2}$ (soit la demi-longueur d'une diagonale).

Notons que l'application $N$ de l'énoncé s'étend naturellement à $\mathbf{C}$ tout entier. En identifiant $\mathbf{C}$ à $\mathbf{R}^2$ au moyen de la $\mathbf{R}$-base $\{1, i\}$, $\mathbf{Z}[i]$ se retrouve identifié à $\mathbf{Z}^2$ et l'observation précédente se traduit ainsi : pour tout élément $z$ de $\mathbf{C}$, il existe un élément $y$ de $\mathbf{Z}[i]$ tel qu'on a $N(x-y) < 1$.

Démontrons à présent que $N$ est bien un stathme euclidien. On vérifie aussitôt que pour tous $z, z' \in \mathbf{C}$ on a $N(z.z') = N(z)N(z')$. Soit $a$ et $b$ des éléments de $\mathbf{Z}[i]$, avec $b \neq 0$. Considérons le quotient $\frac{a}{b} \in \mathbf{C}$. D'après ce qui précède, on peut trouver un élément $q$ de $\mathbf{Z}[i]$ tel que $N\left(\frac{a}{b} - q\right) < 1$. En multipliant par $N(b)$ (qui est strictement positif car $b$ est non nul), on obtient $N(b)N\left(\frac{a}{b} - q\right) < N(b)$ soit encore $N\left(b\frac{a}{b} - bq\right) < N(b)$ d'où finalement $N(a - bq) < N(b)$. Posons alors $r = a - bq$. Comme $a$, $b$ et $q$ sont dans $\mathbf{Z}[i]$, on a $r \in \mathbf{Z}[i]$. Finalement on a $a = bq + r$ et $N(r) < N(b)$.

On a donc bien montré que $\mathbf{Z}[i]$ était un anneau euclidien. □

*Remarque.* Sauf lorsque $\frac{a}{b} \in \mathbf{Z}[i]$ (c'est à dire lorsque la division « tombe juste »), il n'y a jamais unicité de l'élément $q$ de la démonstration précédente, car pour un point donné d'un carré de côté 1 distinct d'un des sommets, il y a toujours au moins deux sommets du carré qui sont à distance $< 1$ de ce point. Par conséquent, la division euclidienne dans $\mathbf{Z}[i]$ n'est pas unique, contrairement à ce qu'il se passe sur $\mathbf{Z}$ ou $\mathbf{K}[X]$ ($\mathbf{K}$ un corps).

Ceci est illustré dans l'exemple ci-dessous.

*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

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

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 $\mathbf{Z}$.

*Démonstration.* L'équivalence entre (2) et (3) a été démontrée comme exemple d'application d'un théorème d'isomorphisme (*cf.* l'exemple qui suit le théorème 48 du chapitre 2).

On a vu que (1)⇒(2) (ou, ce qui revient au même, sa contraposée) vaut en toute généralité dans n'importe quel anneau intègre (*cf.* la proposition 2).

L'implication (4)⇒(3) est laissée à titre d'exercice, et ne fait appel qu'à des raisonnements élémentaires d'arithmétique (qui en particulier ne nécessitent pas d'utiliser $\mathbf{Z}[i]$).

Jusqu'ici, nous n'avons pas utilisé le fait que $\mathbf{Z}[i]$ était euclidien, ou l'une des conséquences arithmétiques « fortes » qui en découlent. On peut démontrer (1)⇒(4) sans faire non plus appel à ces propriétés fortes de $\mathbf{Z}[i]$.

En effet, en ayant remarqué que $p$ n'était ni nul, ni inversible dans $\mathbf{Z}[i]$ (car $N(p) = p^2 \neq 1$) dire que $p$ n'est pas irréductible dans $\mathbf{Z}[i]$ entraîne qu'il existe $z_1, z_2 \in \mathbf{Z}[i]$ non associés à $p$ et tels que $p = z_1 z_2$. En prenant la norme on obtient $p^2 = N(z_1 z_2) = N(z_1)N(z_2)$. Comme il s'agit d'une égalité dans $\mathbf{N}$ et que $N(z_1) = 1$ et $N(z_2) = 1$ sont exclus (car sinon $z_1$ ou $z_2$ serait associé à $p$), la primalité de $p$ entraîne que $N(z_1) = N(z_2) = p$. Soit $(a, b) \in \mathbf{Z}^2$ tel que $z_1 = a + ib$. Alors $p = N(z_1) = a^2 + b^2$.

Pour obtenir le résultat du théorème, il suffit donc de démontrer l'implication (2)⇒(1). C'est ici qu'on applique une des conséquences arithmétiques fortes du fait que $\mathbf{Z}[i]$ est euclidien, à savoir le fait que tout anneau euclidien vérifie la propriété « irréductible=premier » (*cf.* le théorème 10). □

*Remarque.* Il découle du théorème 4 du chapitre 3 que $-1$ est un carré modulo $p$ si et seulement si $p = 2$ ou $p$ est congru à 1 modulo 4.

*Remarque.* Dans un excès d'enthousiasme, on pourrait se laisser aller à penser que pour tout entier strictement positif $n$, ce qui précède se généralise facilement à la caractérisation des nombres premiers qui s'écrivent sous la forme $a^2 + nb^2$, avec $a, b \in \mathbf{Z}$, en utilisant l'anneau $\mathbf{Z}[i\sqrt{n}]$ en lieu et place de $\mathbf{Z}[i]$. De fait, un certain nombre d'arguments se transposent aisément, mais le pas crucial consistant à appliquer la propriété « irréductible=premier » dans $\mathbf{Z}[i]$ fait complètement défaut en général. Déjà pour $n = 3$, il n'est pas vrai en toute généralité que $p$ s'écrit $a^2 + 3b^2$ si et seulement si $-3$ est un carré modulo $p$, à cause de $p = 2$ (c'est vrai si on suppose $p$ impair, sans être immédiat). Notons qu'on a vu dans l'exercice 2.5 que 2 était un exemple d'élément irréductible de $\mathbf{Z}[i\sqrt{3}]$ tel que $2\mathbf{Z}[i\sqrt{3}]$ n'est pas un idéal premier. Pour une solution générale au problème ci-dessus, on pourra consulter l'ouvrage (fabuleux ; vraiment !) *Primes of the form* $x^2 + ny^2$ de David Cox.