Entiers de Gauss

(sujet d'étude XM')

Vincent Lefèvre

1993

Soit $\mathbb{Z}(i) = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}$. $\mathbb{Z}(i)$ est un anneau. On pose :

$$N(a + ib) = a^2 + b^2.$$

a) *Montrer que $N(xy) = N(x)\,N(y)$. En déduire les éléments inversibles de $\mathbb{Z}(i)$.*

On a : $\forall\,(x, y) \in \mathbb{C}^2,\ |xy|^2 = |x|^2\,|y|^2$, donc

$$\boxed{\forall\,(x, y) \in \mathbb{Z}(i)^2,\ N(xy) = N(x)\,N(y).}$$

Si x est inversible : $N(x^{-1}) = \dfrac{N(x.x^{-1})}{N(x)} = \dfrac{1}{N(x)} \in \mathbb{N}^*$, donc $N(x) = 1$.

Les éléments inversibles de $\mathbb{Z}(i)$ sont donc ± 1 et $\pm i$.

b) *Si $x \in \mathbb{Z}(i)$ et si $N(x)$ est un entier premier, montrer que x est irréductible (i.e. $x = \alpha.\beta \Rightarrow \alpha$ ou β inversible). La réciproque est-elle vraie ?*

Soit $x = \alpha\beta$ où $(\alpha, \beta) \in \mathbb{Z}(i)^2$, et $p = N(x) = N(\alpha)\,N(\beta)$. L'un des deux nombres $N(\alpha)$ et $N(\beta)$ est égal à p, et l'autre est égal à 1, car p est premier. Or y est inversible ssi $N(y) = 1$. Donc α ou β est inversible. Donc x est irréductible.

La réciproque est *fausse* : par exemple, 3 est irréductible, mais $N(3) = 9$ n'est pas premier.

Mais si $x = a + ib$ est tel que $ab \neq 0$, alors la réciproque est *vraie* (cf compléments).

c) *Division euclidienne dans $\mathbb{Z}(i)$.*

Soient $x \in \mathbb{Z}(i)$, $y \in \mathbb{Z}(i)^*$. On pose $\frac{x}{y} = u+iv$, où $(u, v) \in \mathbb{Q}^2$. On prend $(u_0, v_0) \in \mathbb{Z}^2$ tel que $|u-u_0| \leqslant \frac{1}{2}$ et $|v-v_0| \leqslant \frac{1}{2}$. Montrer qu'on a : $x = y(u_0+iv_0)+r$ avec $N(r) < N(y)$. Dans quel cas $u_0 + iv_0$ et r sont-ils uniques ?

On a :

$$\frac{r}{y} = \frac{x}{y} - u_0 - iv_0 = (u - u_0) + i(v - v_0),$$

et

$$\frac{N(r)}{N(y)} = N\left(\frac{r}{y}\right) = (u - u_0)^2 + (v - v_0)^2 \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

Donc $\boxed{N(r) < N(y)}$.

Le couple $(u_0 + iv_0, r)$ convient ssi $N(r) < N(y)$, i.e. $(u - u_0)^2 + (v - v_0)^2 < 1$, i.e. (u, v) appartient au disque ouvert de centre (u_0, v_0) et de rayon 1. $(u_0 + iv_0, r)$ est unique ssi $\frac{x}{y} \in \mathbb{Z}(i)$. (Découper le plan en carrés de sommets : $(\frac{m-1}{2}\,;\,\frac{n}{2})$, $(\frac{m}{2}\,;\,\frac{n+1}{2})$, $(\frac{m+1}{2}\,;\,\frac{n}{2})$, $(\frac{m}{2}\,;\,\frac{n-1}{2})$ où m et n sont des entiers tels que $m + n$ est impair.)

d) *En déduire que $\mathbb{Z}(i)$ est principal.*

- $\mathbb{Z}(i)$ est intègre, car $\mathbb{Z}(i) \subset \mathbb{C}$ et $\mathbb{C}$ est un corps.
- Tout idéal $\mathcal{I}$ de $\mathbb{Z}(i)$ est principal :
  Soient $n = \min\limits_{x \in \mathcal{I} - \{0\}} N(x)$ et $a \in \mathcal{I}$ tels que $N(a) = n$. Soient $x \in \mathcal{I}$ et $(u_0 + iv_0, r)$ tels que $x = a(u_0 + iv_0) + r$ avec $N(r) < N(a)$. Or $r \in \mathcal{I}$. Donc $r = 0$, et $x \in a.\mathbb{Z}(i)$, donc $\mathcal{I}$ est principal.

e) *Soit p un nombre premier dans $\mathbb{Z}$. Montrer que p est irréductible ssi il n'existe pas $(a, b) \in \mathbb{N}^2$ tel que $p = a^2 + b^2$.*

- Si $\exists\,(a, b) \in \mathbb{N}^2,\ p = a^2 + b^2$, alors $p = (a + ib)(a - ib)$, et p n'est pas irréductible dans $\mathbb{Z}(i)$.
- Si p n'est pas irréductible dans $\mathbb{Z}(i)$, alors $\exists\,(\alpha, \beta) \in \mathbb{Z}(i)^2,\ p = \alpha\beta$ avec $N(\alpha) > 1$ et $N(\beta) > 1$. Or $N(\alpha)\,N(\beta) = N(p) = p^2$. Donc $N(\alpha) = N(\beta) = p$ (car p est premier), et $p = \mathrm{Re}(\alpha)^2 + \mathrm{Im}(\alpha)^2$.

f) *Montrer que si p est un nombre premier tel que $p \equiv 3\ (mod\ 4)$, alors*

$$a^2 + b^2 \equiv 0\ (mod\ p) \Rightarrow a \equiv 0\ (mod\ p)\ \textit{et}\ b \equiv 0\ (mod\ p).$$

En déduire que tout nombre premier $\geqslant 3$ est irréductible dans $\mathbb{Z}(i)$ ssi $p \equiv 3\ (mod\ 4)$.

Soit p un nombre premier impair. Supposons que $a^2 + b^2 \equiv 0 \pmod p$ et $b \not\equiv 0 \pmod p$. Soit $\alpha = a.b^{-1}$ (dans $\mathbb{Z}/p\mathbb{Z}$). Alors $\alpha^2 = -1$ et $(-\alpha)^2 = -1$.

Les autres éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ peuvent être associés deux par deux de la manière suivante : x et y sont associés ssi $xy = -1$, i.e. $x = -y^{-1}$ (on a $x \neq y$ car -1 a au plus 2 racines carrées). Donc $(p-1)! = (-1)^{(p-3)/2}$. Or $(p-1)! = -1$ (théorème de Wilson). Donc $p \equiv 1 \pmod 4$. Si -1 n'a pas de racine carrée, alors $(p-1)! = (-1)^{(p-1)/2}$ et $p \equiv 3 \pmod 4$.

- Si p est un nombre premier $\geqslant 3$ non irréductible, $\exists\,(a,b) \in \mathbb{N}^2,\ p = a^2 + b^2$ (question e). Or $a^2 \equiv 0$ ou $1 \pmod 4$ et $b^2 \equiv 0$ ou $1 \pmod 4$. Donc $p \not\equiv 3 \pmod 4$.
- Si $p \equiv 1 \pmod 4$, alors $\exists\,\alpha \in \mathbb{N}^*,\ \alpha^2 \equiv -1 \pmod p$ (cf ci-dessus), et $p \mid (\alpha+i)(\alpha-i)$. Si p divise l'un des deux facteurs, alors il divise l'autre (passer aux conjugués), et la différence $2i$, ce qui est impossible. Donc p ne divise aucun des deux facteurs. Donc p n'est pas premier dans $\mathbb{Z}(i)$. Or $\mathbb{Z}(i)$ est principal. Donc p n'est pas irréductible dans $\mathbb{Z}(i)$.

Compléments :

g) Un entier n peut se mettre sous la forme d'une somme de 2 carrés ssi il est de la forme :

$$n = \left(\prod_j p_j^{\alpha_j}\right)\left(\prod_{4k+3 \text{ premier}} (4k+3)^{2\beta_k}\right)$$

où p_j est un nombre premier tel que $p_j \not\equiv 3 \pmod 4$, i.e. les exposants des facteurs premiers de la forme $4k+3$ sont pairs.

Démonstration :

- Si n est de la forme donnée ci-dessus, alors n est une somme de 2 carrés, car si $c = e^2 + f^2$ et $d = g^2 + h^2$, alors

  $$cd = [(e+if)(g+ih)]\,\overline{[(e+if)(g+ih)]} = m^2 + n^2,$$

  et le second terme est un carré.
- Si n n'est pas de la forme donnée ci-dessus, alors il existe $p = 4k+3$ premier d'exposant impair, et si n est somme de 2 carrés, n s'écrit : $n = k^2(a^2+b^2)$ avec $a \wedge b = 1$. Mais d'après la question f (début), $a \equiv 0 \pmod p$ et $b \equiv 0 \pmod p$ car $p \mid a^2 + b^2$, ce qui contredit $a \wedge b = 1$. Donc n n'est pas une somme de 2 carrés.

h) C.N.S. pour que $x \in \mathbb{Z}(i)$ soit irréductible :

Soit $x = a + ib$ tel que $N(x)$ soit un nombre composé (le cas $N(x)$ premier a été traité en b). $N(x)$ est une somme de 2 carrés, donc $N(x)$ est de la forme donnée au début de g.

- Si $N(x)$ n'est pas le carré d'un nombre premier de la forme $4k + 3$:

  Alors il existe c et d, sommes de 2 carrés, tels que $N(x) = cd$. On a : $c = e^2 + f^2$ et $d = g^2 + h^2$. $x\overline{x} = cd = (m+in)(m-in)$ avec $m+in = (e+if)(g+ih)$. Supposons que x soit irréductible. Alors x divise l'un des deux facteurs ($m+in$ par exemple). On a : $\alpha x = m + in$ avec $N(\alpha) = 1$ car $N(m + in) = N(x)$. Donc

  $$x = \alpha^{-1}(m + in) = \alpha^{-1}(e + if)(g + ih).$$

  Contradiction. Donc x est *réductible*.

- Si $N(x)$ est le carré d'un nombre premier de la forme $4k + 3$:

  Soit $x = \alpha\beta$. $N(\alpha) \neq p$ car $N(\alpha)$ est une somme de 2 carrés, mais pas p. Donc x est *irréductible*.

  On a de plus, d'après la question f : $a \equiv 0 \pmod{p}$ et $b \equiv 0 \pmod{p}$, car $a^2 + b^2 \equiv 0 \pmod{p}$. Donc x est de la forme $i^s p$.

Conclusion :

Soit $x = a + ib \in \mathbb{Z}(i)$ tel que $N(x) > 1$. x est *irréductible* ssi on a l'une des deux conditions suivantes :

- $N(x)$ est un nombre premier (alors $ab \neq 0$).
- $N(x)$ est le carré d'un nombre premier de la forme $4k + 3$ (alors $ab = 0$).