Corrigé Devoir à la maison Arithmétique et algèbre commutative 19 mars 2013

Le but de ce devoir est d'étudier certain propriétés fondamentales d'un anneau euclidien assez similaire à $\mathbf{Z}[\mathbf{i}]$, à savoir l'anneau des entiers d'Eisenstein.

1. On désigne par $\mathbf{j}$ le nombre complexe $e^{\frac{2\pi}{3}\mathbf{i}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}\mathbf{i}$, qui vérifie $\mathbf{j}^3 = 1$.

a. Donner une décomposition du polynôme $X^3 - 1$ comme produit de deux facteurs dans $\mathbf{Z}[X]$.

$\surd$ *On a le facteur évident* $X-1$*, et par division euclidienne on obtient* $X^3-1 = (X-1)(X^2+X+1)$.

b. Indiquer lequel des deux facteurs possède $\mathbf{j}$ comme racine; on nomme F ce facteur.

$\surd$ *Le facteur* $X-1$ *n'a que* 1 *comme racine, donc c'est* $F = X^2+X+1$ *qui possède* $\mathbf{j}$ *comme racine. On peut vérifier cela par un calcul explicite, mais ce n'est pas nécessaire: comme* $0 = \mathbf{j}^3 - 1 = (\mathbf{j}-1)(\mathbf{j}^2+\mathbf{j}+1)$ *et* $\mathbf{Z}[\mathbf{j}]$ *est un anneau intègre (car sous-anneau de* $\mathbf{C}$*) il est clair que* $\mathbf{j}^2+\mathbf{j}+1 = 0$.

c. L'application $f : \mathbf{Z}[X] \to \mathbf{C}$ qui à un polynôme P associe sa valeur $P[X := \mathbf{j}]$ en $\mathbf{j}$ est un morphisme d'anneaux. Montrer que $\ker f$ est l'idéal principal de $\mathbf{Z}[X]$ engendré par F.

$\surd$ *Dans la question précédente on a vu que* $F = X^2+X+1 \in \ker f$*. Or* F *est unitaire, donc d'après la proposition 1.5.15,* F *sera générateur de* $\ker f$ *si on peut montrer que* $\ker f$ *ne contient pas de polynôme de degré* 0 *ou* 1*. Mais comme* $\mathbf{j}$ *n'est pas réel,* $f(a+bX) = a+b\mathbf{j}$ *n'est nul que si* $a, b = 0$*, donc* $\ker f$ *ne contient pas de tels polynômes. Une autre preuve possible est de montrer directement que si* $P \in \mathbf{Z}[X]$ *possède* $\mathbf{j}$ *comme racine, alors* P *est divisible par* F*. Le conjugué complexe* $\overline{\mathbf{j}} = \mathbf{j}^2$ *sera aussi racine de* P*, car l'évaluation en* $\overline{z}$ *d'un polynôme à coefficients réel est le conjugué complexe de son évaluation en* z*. Ainsi* P *est divisible dans* $\mathbf{C}[X]$ *par les facteurs* $X-\mathbf{j}$ *et* $X-\mathbf{j}^2$ *qui sont premiers entre eux, et donc par* $(X-\mathbf{j})(X-\mathbf{j}^2) = X^2-(\mathbf{j}+\mathbf{j}^2)+\mathbf{j}^3 = X^2+X+1 = F$*. Mais le quotient* P/F *est à coefficients entiers, donc* P *est aussi divisible par* F *dans* $\mathbf{Z}[X]$.

2. L'anneau des entiers d'Eisenstein est $\mathbf{Z}[\mathbf{j}]$, le plus petit sous-anneau de $\mathbf{C}$ contentant l'élément $\mathbf{j}$.

a. Montrer que $\mathbf{Z}[\mathbf{j}] = \{\, a+\mathbf{j}b \mid a, b \in \mathbf{Z} \,\}$, et exprimer la multiplication sous cette forme, c'est-à-dire écrire $(a+\mathbf{j}b) \times (c+\mathbf{j}d) = e+\mathbf{j}f$ pour certaines expressions e, f (aux valeurs dans $\mathbf{Z}$).

$\surd$ *Un sous-anneau de* $\mathbf{C}$ *qui contient* $\mathbf{j}$ *doit aussi contenir tout élément de* $\mathbf{Z}[\mathbf{j}]$*; une fois montré que cet ensemble est un sous-anneau, c'est-à-dire fermé pour l'addition et pour la multiplication car il contient* $1 = 1+0\mathbf{j}$*, il sera donc certainement le plus petit sous-anneau contenant* $\mathbf{j}$*. Or en utilisant* $\mathbf{j}^2 = -1-\mathbf{j}$ *on a* $(a+\mathbf{j}b) \times (c+\mathbf{j}d) = ac+(ad+bc)\mathbf{j}+bd\mathbf{j}^2 = (ac-bd)+(ad+bc-bd)\mathbf{j}$*, donc l'ensemble* $\{\, a+\mathbf{j}b \mid a, b \in \mathbf{Z} \,\}$ *est fermé pour la multiplication; il l'est aussi pour l'addition.*

b. Montrer que $\mathbf{Z}[\mathbf{j}]$ est stable par la conjugaison complexe, et exprimer $\overline{a+\mathbf{j}b}$ sous la forme $a'+\mathbf{j}b'$.

$\surd$ *On a* $\overline{\mathbf{j}} = \mathbf{j}^2 = -1-\mathbf{j}$ *et évidemment* $\overline{1} = 1$*, donc* $\overline{a+\mathbf{j}b} = (a-b)-\mathbf{j}b$.

c. On définit $N : \mathbf{Z}[\mathbf{j}] \to \mathbf{Z}$ par $N(x) = x\overline{x} = |x|^2$, application appelée la norme de $\mathbf{Z}[\mathbf{j}]$. Montrer que effectivement $N(x) \in \mathbf{Z}$ pour $x \in \mathbf{Z}[\mathbf{j}]$, et exprimer $N(a+\mathbf{j}b)$ en termes de $a, b \in \mathbf{Z}$.

$\surd$ $N(a+\mathbf{j}b) = (a+\mathbf{j}b)((a-b)-\mathbf{j}b) = (a(a-b)-b(-b))+(a(-b)+b(a-b)-b(-b))\mathbf{j}$*, ce qui donne*

$$N(a+\mathbf{j}b) = a^2 - ab + b^2,$$

car le coefficient de $\mathbf{j}$ *se simplifie à* 0*. Cette expression est clairement dans* $\mathbf{Z}$ *pour* $a, b \in \mathbf{Z}$.

d. Montrer que $N(x) \geq 0$ et $N(x) \not\equiv 2 \pmod 3$ pour tout $x \in \mathbf{Z}[\mathbf{j}]$.

$\surd$ *Considérant* x *comme nombre complexe on a* $N(x) = |x|^2 \geq 0$*. Si on réduit l'expression* a^2-ab+b^2 *modulo* 3*, sa valeur se calcule selon les classes modulo* 3 *de* a *et de* b*, et dans les* 9 *cas on ne trouve que les classes de* 0 *ou* 1 *comme valeur, selon le tableau suivant :*

$$\begin{array}{c|ccc} & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{array}$$

e. Montrer que N est multiplicatif: $N(xy) = N(x)N(y)$ pour tout $x, y \in \mathbf{Z}[\mathbf{j}]$.

$\surd$ $N(xy) = xy\overline{xy} = x\overline{x}y\overline{y} = N(x)N(y)$.

f. Trouver l'ensemble $\mathbf{Z}[\mathbf{j}]^\times$ des éléments inversibles dans $\mathbf{Z}[\mathbf{j}]$.

√ *Si $xy = 1$ dans $\mathbf{Z}[\mathbf{j}]$ on a d'après la question précédente $N(x)N(y) = 1$ avec $N(x), N(y) \in \mathbf{N}$, donc forcément $N(x) = 1 = N(y)$. En écrivant $a^2 - ab + b^2 = (a-b)^2 + ab = (a+b)^2 - ab$ on voit facilement que l'équation $a^2 - ab + b^2 = 1$ avec $a, b \in \mathbf{Z}$ ne possède que les 6 solutions $(a, b) \in \{(1,0), (1,1), (0,1), (-1,0), (-1,-1), (0,-1)\}$ qui correspondent à*

$$\mathbf{Z}[\mathbf{j}]^\times = \{1, 1+\mathbf{j}, \mathbf{j}, -1, -1-\mathbf{j}, -\mathbf{j}\} = \{\, e^{\frac{2\mathbf{i}\pi}{6}k} \mid 0 \le k < 6 \,\}.$$

3. On montrera maintenant que $\mathbf{Z}[\mathbf{j}]$ est une anneau euclidien, avec N comme stathme.

a. Trouver géométriquement le lieu des $z \in \mathbf{C}$ tel que la distance $|a + \mathbf{j}b - z|$, avec $a, b \in \mathbf{Z}$, soit minimale pour $a = b = 0$ (aucun point de $\mathbf{Z}[\mathbf{j}]$ n'est plus proche de z que $0 \in \mathbf{C}$ ne l'est). Conclure qu'un tel z vérifie en particulier $|z| < 1$.

√ *Les z tels que la distance $|z|$ vers $0+0\mathbf{j}$ n'est pas plus grand que la distance $|1-z|$ vers $1+0\mathbf{j}$ sont ceux dans le demi-plan à gauche de la droite médiatrice $\operatorname{Re} z = \frac{1}{2}$, la droite elle-même incluse. Faisant pareillement pour les autres éléments de $\mathbf{Z}[\mathbf{j}]^\times$ on trouve 6 demi-plans fermés contenant l'origine, dont l'intersection est un hexagone (sommets, côtés et intérieure). Les sommets de l'hexagone sont les intersections de deux médiatrices, tel le point $\frac{1}{2} + \frac{1}{2\sqrt{3}}\mathbf{i}$ qui est à distances égales de 0, de 1, et de $1 + \mathbf{j} = \frac{1}{2} + \frac{\sqrt{3}}{2}\mathbf{i}$, la distance étant $\frac{1}{\sqrt{3}}$. En particulier cet hexagone est contenu dans le disque autour de 0 de rayon $\frac{1}{\sqrt{3}} < 1$. Tout autre point $z \in \mathbf{Z}[\mathbf{j}]$ a $N(x) > 1$ et donc $N(x) \ge 3$, et donc distance $|z| \ge \sqrt{3}$ de l'origine, ce qui est plus de 2 fois la distance vers l'origine pour tout point de l'hexagone; ces points ci sont donc forcément plus proches de l'origine que de z. En conclusion, les points de l'hexagone sont ceux pour qui la distance vers les $z \in \mathbf{Z}[\mathbf{j}]$ est minimale pour $z = 0$.*

b. Soit $x, y \in \mathbf{Z}[y]$ avec $y \neq 0$, et $q \in \mathbf{Z}[\mathbf{j}]$ tel que $|q - \frac{x}{y}| < 1$ (où $\frac{x}{y}$ est calculé dans $\mathbf{C}$). Montrer que $r = x - qy \in \mathbf{Z}[\mathbf{j}]$ vérifie $N(r) < N(y)$.

√ *L'inégalité donnée entraîne $|r| = |y|\,|\frac{x}{y} - q| < |y|\,1 = |y|$, et donc $N(r) = |r|^2 < |y|^2 = N(y)$.*

c. Conclure des deux questions précédentes que $\mathbf{Z}[\mathbf{j}]$ est une anneau euclidien, avec N comme stathme. D'après le cours cela entraîne que $\mathbf{Z}[\mathbf{j}]$ est un anneau principal, et donc factoriel.

√ *Soit $x, y \in \mathbf{Z}[y]$ avec $y \neq 0$, et soit $q \in \mathbf{Z}[\mathbf{j}]$ un élément pour lequel $|\frac{x}{y} - q|$ atteint sa valeur minimale. (L'existence d'un tel élément est intuitivement évident car $\mathbf{Z}[\mathbf{j}]$ est une partie discrète de $\mathbf{C}$, mais c'est un peu subtile à justifier rigoureusement. En fait en posant $r = |\frac{x}{y}|$ l'intersection de $\mathbf{Z}[\mathbf{j}]$ avec le disque fermé (donc compact) $\{\, z \in \mathbf{C} \mid |\frac{x}{y} - z| \le r + 1 \,\}$ est fini et non vide (il contient 0), et $|\frac{x}{y} - q|$ atteint sa valeur minimale pour q dans cet ensemble.) Comme $\mathbf{Z}[\mathbf{j}]$ est globalement invariant pour la translation par $-q$, le nombre complexe $z_0 = \frac{x}{y} - q$ a la propriété que la distance $|z_0 - p|$ pour $p \in \mathbf{Z}[\mathbf{j}]$ atteint son minimum pour $p = 0$, c'est-à-dire z_0 est dans l'hexagone décrit dans la question a. En particulier $|z_0| < 1$, c'est-à-dire $|\frac{x}{y} - q| < 1$. En posant $r = x - qy \in \mathbf{Z}[\mathbf{j}]$ la question précédente nous donne $N(r) < N(y)$. Donc si on prend les nombres $q, r \in \mathbf{Z}[\mathbf{j}]$ comme quotient et reste de la division de x par y, la condition pour que N soit stathme euclidien est vérifiée.*

d. Indiquer comment on peut trouver *effectivement* pour x, y donnés des éléments q, r comme décrits dans la question b (il n'est pas demandé de trouver r tel que $N(r)$ soit le plus petit possible, mais la méthode pour trouver r doit être tel qu'on puisse le programmer en ordinateur).

√ *Pour la preuve que N est un stathme, il n'est pas nécessaire d'utiliser comme quotient q l'élément le plus proche de $\frac{x}{y}$, il suffit qu'il soit à distance < 1. Le plus simple est alors d'écrire $\frac{x}{y} = \alpha + \mathbf{j}\beta$ pour $\alpha, \beta \in \mathbf{Q}$ et d'arrondir α, β individuellement vers l'entier le plus proche, disons $a, b \in \mathbf{Z}$ respectivement. Alors $|\frac{x}{y} - (a + \mathbf{j}b)| = |(\alpha - a) + \mathbf{j}(\beta - b)|$ et il s'agit de montrer que c'est toujours < 1. Or $|c + \mathbf{j}d|^2 = c^2 - cd + d^2$ par le même calcul que dans la question **2***c* (mais maintenant avec $c, d \in \mathbf{Q}$), et on voudrait montrer que c'est < 1 quand $|c|, |d| \le \frac{1}{2}$; mais on a alors pour les termes individuels $c^2, -cd, d^2 \le \frac{1}{4}$, et donc $|c+\mathbf{j}d|^2 = c^2 - cd + d^2 \le \frac{3}{4} < 1$ comme voulu. Voici la procédure de calcul complète. Si $x = x_0 + \mathbf{j}x_1, y = y_0 + \mathbf{j}y_1$ avec $x_0, x_1, y_0, y_1 \in \mathbf{Z}$, sachant que $\frac{x}{y} = \frac{x\overline{y}}{y\overline{y}} = \frac{(x_0y_0 - x_0y_1 + x_1y_1) + \mathbf{j}(x_1y_0 - x_0y_1)}{y_0^2 - y_0y_1 + y_1^2}$ on pose $\alpha = \frac{x_0y_0 - x_0y_1 + x_1y_1}{y_0^2 - y_0y_1 + y_1^2}$ et $\beta = \frac{x_1y_0 - x_0y_1}{y_0^2 - y_0y_1 + y_1^2}$, nombres rationnels pour lesquels on calcule ensuite les entiers $a = \lfloor \alpha + \frac{1}{2} \rfloor$ et $b = \lfloor \beta + \frac{1}{2} \rfloor$ les plus proches (avec arrondi vers le bas en cas de ex aequo). Alors le quotient est $q = a + \mathbf{j}b$, et le reste est $r = x - qy \in \mathbf{Z}[\mathbf{j}]$. La preuve de la question précédente, adaptée à ce choix de q, r mais qui vérifie toujours $|\frac{x}{y} - q| < 1$, montre que c'est une division euclidienne avec stathme N. L'opération de arrondir un nombre rationnel vers l'entier le plus proche peut facilement être exprimée en termes d'opérations arithmétiques sur numérateur et dénominateur. Le point essentiel de cette question*

est d'éviter comme ingrédient la recherche de l'élément le plus proche dans $\mathbf{Z}[\mathbf{j}]$*, car décrit ainsi, cela fait appel à un nombre infini de comparaisons.*

4. On décrira les éléments irréductibles de l' anneau factoriel $\mathbf{Z}[\mathbf{j}]$. Argumenter successivement :

a. Si $x \in \mathbf{Z}[\mathbf{j}]$ est tel que $N(x) \in \mathbf{N}$ est un nombre premier, alors x est irréductible dans $\mathbf{Z}[\mathbf{j}]$.

√ *On a vu que les éléments inversibles de* $\mathbf{Z}[\mathbf{j}]$ *sont ceux de norme* 1*, et* 0 *est le seul élément de norme* 0*. Si* $y, z\mathbf{Z}[\mathbf{j}]$ *sont non nuls et non inversibles on a* $N(yz) = N(y)N(z)$*, un produit de deux nombres* > 1 *qui est donc composé. Il est alors impossible d'avoir une telle décomposition* $x = yz$ *si* $N(x)$ *est un nombre premier. Un tel* x*, n'étant également ni nul ni inversible, est irréductible.*

b. Si réciproquement $x \in \mathbf{Z}[\mathbf{j}]$ est irréductible, on a deux possibilités : soit $N(x)$ est un nombre premier, soit x est lui même associé dans $\mathbf{Z}[\mathbf{j}]$ à un nombre premier p, et dans ce cas $N(x) = p^2$. Indication: utiliser que $N(x) = x\overline{x}$ dans $\mathbf{Z}[\mathbf{j}]$, et le fait que $\mathbf{Z}[\mathbf{j}]$ est un anneau factoriel.

√ *Comme la conjugaison complexe induit un automorphisme de* $\mathbf{Z}[\mathbf{j}]$*, le fait que* x *est irréductible implique que* $\overline{x}$ *l'est aussi. Alors* $N(x) = x\overline{x}$ *est une factorisation de* $N(x)$ *dans* $\mathbf{Z}[\mathbf{j}]$*. Comme* $\mathbf{Z}[\mathbf{j}]$ *est factoriel, c'est la seule factorisation à l'ordre des facteurs et à association près, donc si* x *n'est pas associé à un élément de* $\mathbf{Z}$*, alors* $N(x)$ *ne possède aucune factorisation (non triviale) dans* $\mathbf{Z}$*, et c'est donc un nombre premier. Si par contre* x *est associé à un nombre* $n \in \mathbf{Z}$ *(qu'on peut supposer positif car* n *est associé à* $-n$*), alors* $\overline{x}$ *est aussi associé à* n*, et la décomposition de* $N(x)$ *devient* $N(x) = n^2$ *(il ne reste pas de facteur* -1 *dans la décomposition, car* $N(x) \in \mathbf{N}$*). Mais comme c'est la seule décomposition dans* $\mathbf{N}$ *de* $N(x)$*, il est nécessaire que* n *soit un nombre premier.*
Une toute autre approche est de considérer l'idéal $x\mathbf{Z}[\mathbf{j}]$ *de* $\mathbf{Z}[\mathbf{j}]$ *engendré par* x*. Comme* $\mathbf{Z}[\mathbf{j}]$ *est factoriel l'élément irréductible* x *est aussi premier, donc* $x\mathbf{Z}[\mathbf{j}]$ *un idéal premier. Il coupe alors le sous-anneau* $\mathbf{Z}$ *en un idéal premier de celui-ci, c'est-à-dire un idéal de la forme* $p\mathbf{Z}$ *avec* p *premier, ou* $\{0\}$*. Mais cette dernière possibilité n'est est pas une, car* $0 \neq N(x) = x\overline{x} \in x\mathbf{Z}[\mathbf{j}] \cap \mathbf{Z}$*. Si* x *n'est pas lui-même associé à ce nombre premier* p*, alors* $N(x)$ *est un diviseur strict et distinct de* 1 *de* $N(p) = p^2$*, et cela ne laisse que* $N(x) = p$ *comme possibilité.*

c. Tout nombre premier $p \equiv 2 \pmod 3$ reste irréductible en tant que élément de $\mathbf{Z}[\mathbf{j}]$.

√ *Comme* p *n'est ni* 0 *ni inversible dans* $\mathbf{Z}[\mathbf{j}]$*, il possède au moins un facteur irréductible* x *dans* $\mathbf{Z}[\mathbf{j}]$*, et on aura alors que* $N(x)$ *divise* $N(p) = p^2$ *dans* $\mathbf{Z}$ *(d'après la multiplicativité de* N*). Mais* $N(x) = p$ *est impossible (question* $\mathbf{1}d$*) donc on doit avoir* $N(x) = p^2$*. Alors* x *est associé à* p *d'après la question précédente, donc* p *est, comme* x*, irréductible dans* $\mathbf{Z}[\mathbf{j}]$.

d. Réciproquement, si p est un nombre premier qui reste irréductible en tant que élément de $\mathbf{Z}[\mathbf{j}]$:

i. alors l'idéal principal $p\mathbf{Z}[\mathbf{j}]$ de $\mathbf{Z}[\mathbf{j}]$ engendré par p est un idéal premier (et maximal),

√ *Un élément irréductible dans un anneau factoriel est premier (théorème 2.2.10(ii)), donc engendre un idéal premier. (Cet idéal est aussi maximal d'après proposition 2.3.9.)*

ii. l'idéal principal de $(\mathbf{Z}/p\mathbf{Z})[X]$ engendré par la réduction $\overline{F}$ modulo p du polynôme F de la question $\mathbf{1}b$ est premier (et maximal),

√ *D'après le point précédent, le quotient* $\mathbf{Z}[\mathbf{j}]/p\mathbf{Z}[\mathbf{j}]$ *est un anneau intègre. Comme* F *engendre le noyau du morphisme* $f : \mathbf{Z}[X] \to \mathbf{C}$ *de la première partie, donc l'image est* $\mathbf{Z}[j]$*, on a* $\mathbf{Z}[j] \cong \mathbf{Z}[X]/(F)$ *par le théorème d'isomorphisme (1.3.5). Dans la correspondance entre idéaux de* $\mathbf{Z}[X]/(F)$ *est les idéaux de* $\mathbf{Z}[X]$ *contenant* (F) *(1.3.4), l'idéal* $pZ\mathbf{j}$ *correspond à* $(F, p) = (F) + p\mathbf{Z}[X]$*, donc l'anneau intègre* $\mathbf{Z}[\mathbf{j}]/p\mathbf{Z}[\mathbf{j}]$ *est isomorphe à* $\mathbf{Z}[X]/(F, p)$*. Ce quotient peut aussi être obtenue en formant d'abord le quotient par* $p\mathbf{Z}[X]$*, ce qui donne* $(\mathbf{Z}/p\mathbf{Z})[X]$*, et ensuite le quotient de celui-ci par l'image de* (F, p)*, qui est l'idéal principal* $(\overline{F})$ *de la question actuelle. Du coup on a* $\mathbf{Z}[\mathbf{j}]/p\mathbf{Z}[\mathbf{j}] \cong (\mathbf{Z}/p\mathbf{Z})[X]/(\overline{F})$*. Le quotient à gauche étant intègre (et même un corps), c'est aussi le cas à droite, donc l'idéal* $(\overline{F})$ *de* $(\mathbf{Z}/p\mathbf{Z})[X]$ *est premier (et même maximal).*

iii. ce polynôme $\overline{F}$ est irréductible dans $(\mathbf{Z}/p\mathbf{Z})[X]$,

√ *L'élément* $\overline{F}$ *qui engendre l'idéal premier* $(\overline{F})$ *est premier, donc irréductible (2.2.7).*

iv. le groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^\times$ ne possède pas d'éléments d'ordre 3,

√ *Un tel élément* a *d'ordre* 3 *vérifie* $a^3 = 1$ *dans* $\mathbf{Z}/p\mathbf{Z}$ *mais* $a \neq 1$*; alors* a *est racine de* $X^3 - 1 = (X-1)(X^2+X+1) = (X-1)\overline{F}$*, mais pas de la facteur* $X - 1$*, donc* a *est racine de* $\overline{F}$*. Mais on vient de voir que* $(\overline{F})$ *est irréductible, et n'est pas de degré* 1*, donc il ne possède en particulier pas de racines (une racine* a *donnerait un facteur* $X - a$ *de* $\overline{F}$*).*

v. en conclusion, $p \equiv 2 \pmod 3$.

√ *Le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est toujours cyclique (1.5.10) et d'ordre $p-1$; donc si cet ordre est divisible par 3, alors ce groupe possède un élément d'ordre 3, ce qu'on vient d'exclure. Donc $p \not\equiv 1 \pmod 3$. Le seul premier $p \equiv 0 \pmod 3$ est $p = 3$, mais dans $\mathbf{Z}/3\mathbf{Z}$ on a $X^3 - 1 = (X-1)^3$ (1.2.10), donc $\overline{F} = (X-1)^2$, ce qui n'est pas irréductible. Il ne reste que $p \equiv 2 \pmod 3$.*

e. Conclure que tout nombre premier $p \not\equiv 2 \pmod 3$ s'écrit comme la norme $N(x)$ d'un élément irréductible $x \in \mathbf{Z}[\mathbf{j}]$.

√ *Par la contraposée de ce qu'on vient de démontrer, un nombre premier $p \not\equiv 2 \pmod 3$ n'est pas irréductible dans $\mathbf{Z}[j]$. Un facteur irréductible x de p dans $\mathbf{Z}[j]$ n'y est donc pas associé à p, et d'après la question b, $N(x)$ divise p^2 sans être égal à p^2, ni à 1 (car x n'est pas inversible); $N(x) = p$.*

5. La caractérisation des irréductibles de $\mathbf{Z}[\mathbf{j}]$ permettra de caractériser l'ensemble $\{\, N(x) \mid x \in \mathbf{Z}[\mathbf{j}] \,\}$.

a. Montrer que si $N(a + \mathbf{j}b)$ est divisible par un premier $p \equiv 2 \pmod 3$, alors a, b sont chacun divisible par p (et $N(a + \mathbf{j}b)$ donc divisible par p^2). [Considérer la factorisation de $a + \mathbf{j}b$.]

√ *Si l'on considère une factorisation de $a + \mathbf{j}b$ dans $\mathbf{Z}[j]$, la multiplicativité de N et le fait que $\mathbf{Z}$ est factoriel entraînent que l'un au moins des facteurs irréductibles, disons x, vérifie $p \mid N(x)$ dans $\mathbf{Z}$. Mais comme $p \equiv 2 \pmod 3$, cela n'est possible que si x est associé à p, donc $a + \mathbf{j}b$ est divisible dans $\mathbf{Z}[j]$ par p, ce qui veut dire que a, b sont chacun divisible par p (et $N(a+\mathbf{j}b) = a^2 - ab + b^2$ est divisible par p^2). Un autre argument pour trouver que p divise $a + \mathbf{j}b$ dans $\mathbf{Z}[\mathbf{j}]$ est de dire que p reste irréductible dans $\mathbf{Z}[\mathbf{j}]$ (car $p \equiv 2 \pmod 3$) et divise $N(a+\mathbf{j}b) = (a+\mathbf{j}b)(a-\mathbf{j}b)$, donc il divise l'un des facteurs au moins; mais $p \mid a + \mathbf{j}b$ est équivalent par conjugaison complexe à $p \mid a - \mathbf{j}b$, donc il est nécessaire que p divise les deux facteurs.*

b. Montrer qu'un entier $n > 0$ s'écrit $n = N(x)$ pour $x \in \mathbf{Z}[\mathbf{j}]$ si et seulement si pour tout nombre premier $p \equiv 2 \pmod 3$, la multiplicité de p dans la factorisation (dans $\mathbf{Z}$) de n est paire.

√ *La question précédente montre que pour tout nombre premier $p \equiv 2 \pmod 3$ qui divise n, on a $p \mid x$ dans $\mathbf{Z}[\mathbf{j}]$ et $p^2 \mid n$ dans $\mathbf{Z}$. Si c'est le cas $n/p^2 = N(x/p)$, ce qui permet de montrer par récurrence que la multiplicité de p dans la factorisation de n est paire. La condition donnée est donc nécessaire. Supposons cette condition vérifiée pour tous ces nombres premiers, ce qui veut dire que dans la factorisation (dans $\mathbf{Z}$) de n on peut regrouper les occurrences de ce type de nombres premiers par paires (on laisse les autre facteurs premiers seuls). Pour montrer que la condition est suffisante, il suffit d'écrire chacun des facteurs ainsi obtenus comme norme d'un élément de $\mathbf{Z}[\mathbf{j}]$, en utilisant la multiplicativité de la norme. C'est évidemment possible pour les facteurs $p^2 = N(p)$. Les facteurs restants sont de nombres premiers $p \not\equiv 2 \pmod 3$, et pour ceux-ci la question **4***e* fournit une écriture $p = N(x)$, ce qui termine la démonstration.*

Fin.