Devoir à la maison Arithmétique et algèbre commutative fin mars 2013

Ce devoir est à remettre aux TD le 2 avril 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 $\mathbf{Z}[X]$.
- *b.* Indiquer lequel des deux facteurs possède $\mathbf{j}$ comme racine; on nomme F ce facteur.
- *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.

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 $\mathbf{Z}$).
- *b.* Montrer que $\mathbf{Z}[\mathbf{j}]$ est stable par la conjugaison complexe, et exprimer $\overline{a + \mathbf{j}b}$ sous la forme $a' + \mathbf{j}b'$.
- *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 $a, b \in \mathbf{Z}$.
- *d.* Montrer que $N(x) \geq 0$ et $N(x) \not\equiv 2 \pmod 3$ pour tout $x \in \mathbf{Z}[\mathbf{j}]$.
- *e.* Montrer que N est multiplicatif: $N(xy) = N(x)N(y)$ pour tout $x, y \in \mathbf{Z}[\mathbf{j}]$.
- *f.* Trouver l'ensemble $\mathbf{Z}[\mathbf{j}]^\times$ des éléments inversibles dans $\mathbf{Z}[\mathbf{j}]$.

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 minimal 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 $|z| < 1$.
- *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 $N(r) < N(y)$.
- *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.
- *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).

4. On décrira ses 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 $\mathbf{Z}[\mathbf{j}]$.
- *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.
- *c.* Tout nombre premier $p \equiv 2 \pmod 3$ reste irréductible en tant que élément de $\mathbf{Z}[\mathbf{j}]$.
- *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),
  - *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 **1***b* est premier (et maximal),
  - *iii.* ce polynôme $\overline{F}$ est irréductible dans $(\mathbf{Z}/p\mathbf{Z})[X]$,
  - *iv.* le groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^\times$ ne possède pas d'éléments d'ordre 3,
  - *v.* en conclusion, $p \equiv 2 \pmod 3$.
- *e.* Conclure que tout nombre premier $p \not\equiv 2 \pmod 3$ s'écrit comme la norme $N(x)$ d'un élément irréductible $x \in \mathbf{Z}[\mathbf{j}]$.

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 $a + \mathbf{j}b$.]
- *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.

Fin.