Exercices d'Algèbre 3
Bernd Ammann, 2006–2007
Feuille 9 13 novembre 2006

---

1 Soit A l'anneau $\mathbb{Z}[i]$, et soit $p \in \mathbb{N}$, $p > 2$, p premier. Montrer qu'on a l'équivalence entre

(i) p est réductible dans $\mathbb{Z}[i]$,

(ii) il existe $x \in \mathbb{Z}[i]$ avec $|x|^2 = p$,

(iii) $p \equiv 1 \mod 4$.

(iv) $-\bar{1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$,

2 Montrer que les éléments irréductibles dans $\mathbb{Z}[i]$ sont

- les nombres premiers p tels que $p \equiv 3 \mod 4$ et leurs associés,
- les éléments $z \in \mathbb{Z}[i]$ tels que $|z|^2 = 2$,
- les éléments $z \in \mathbb{Z}[i]$ tels que $|z|^2 = p$ où p est un premier, $p \equiv 1 \mod 4$.

3 Décomposer $8 + 6i$, $69 + 45i$, $26 + 65i$ en facteurs irréductibles dans $\mathbb{Z}[i]$.

4 Décomposer 260 en facteurs irréductibles dans $\mathbb{Z}[i]$. En déduire que 260 est la somme de deux carrés.

5 Calculer les pgcds dans $\mathbb{Z}[i]$ suivants: $pgcd(14-7i, 2-i)$, $pgcd(26+65i, 34+51i)$, $pgcd(69+45i, 12+18i)$.

6 Montrer que l'anneau $\mathbb{Z}[i\sqrt{2}]$ admet un algorithme euclidien avec le degré

$$d(a + bi\sqrt{2}) = a^2 + 2b^2.$$

7 Soit n un élément de $\mathbb{Z}$, non carré d'un entier. Dans le cas $n < 0$ nous définissions $\sqrt{n} := i\sqrt{|n|}$. On met (pour $n < 0$ ou $n > 0$)

$$\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$$

et

$$d : \mathbb{Z}[\sqrt{n}] \to \mathbb{N}, \qquad d(a + b\sqrt{n}) := |a^2 - b^2 n|.$$

(a) Montrer

$$\forall x, y \in \mathbb{Z}[\sqrt{n}] : d(xy) = d(x)d(y).$$

(b) Montrer que $\mathbb{Z}[\sqrt{n}]$ est un anneau commutatif, unitaire et intègre. Détérminer les éléments inversibles de $\mathbb{Z}[\sqrt{n}]$.

(c) Montrer que dans $\mathbb{Z}[\sqrt{n}]$, 2 ne divise ni $n + \sqrt{n}$ ni $n - \sqrt{n}$.

(d) Montrer que s'il n'existe pas $\alpha \in \mathbb{Z}[\sqrt{n}]$ vérifiant $d(\alpha) = 2$, alors 2 est irréductible dans $\mathbb{Z}[\sqrt{n}]$. En déduire que dans ce cas $\mathbb{Z}[\sqrt{n}]$ n'est pas principal.

(e) Montrer que si $n \leq -3$, il n'existe pas d'élément $\alpha \in \mathbb{Z}[\sqrt{n}]$ avec $d(\alpha) = 2$.

(f) Supposons maintenant que n est de la forme $4k + 1$ ($k \in \mathbb{Z}$). Montrer que $d(\alpha) \neq 2$ pour tout $\alpha \in \mathbb{Z}[\sqrt{n}]$.
Indication: Soit $\alpha = x + y\sqrt{n}$ un élément de $\mathbb{Z}[\sqrt{n}]$. Montrer que si $d(\alpha) = 2$, alors $x^2 - y^2 + 2$ est divisible par 4. En déduire une contradiction.

(g) Donner quelques sous-anneaux unitaires de $\mathbb{C}$ qui ne sont pas factoriels.