Anneaux et Arithmétique - CC2
L3, semestre 2 (2012-2013)
Université Rennes I

Contrôle continu 2

Durée : 1h. Les documents ne sont pas autorisés.

Exercice 1.

Soit A un anneau commutatif unitaire. Soient $I, J \subset A$ des idéaux de A.
1) Montrer que $I \cap J$ et $I + J = \{i + j \ / \ i \in I, j \in J\}$ sont des idéaux de A.
2) Montrer que l'idéal IJ engendré par les éléments de A de la forme ij avec $i \in I$ et $j \in J$ est contenu dans $I \cap J$.
3) On suppose que $I + J = A$. Montrer que $IJ = I \cap J$.

Problème

Soit $\mathbb{Z}[i] = \{a + ib, \ (a, b) \in \mathbb{Z}^2\}$.
1) Montrer que $\mathbb{Z}[i]$ est un anneau commutatif unitaire, et qu'il est intègre.
2) Pour $z = a + ib \in \mathbb{Z}[i]$, on pose $N(z) = a^2 + b^2$. Montrer que pour $z, z' \in \mathbb{Z}[i]$, $N(zz') = N(z)N(z')$.
3) Montrer que $z \in \mathbb{Z}[i]$ est inversible si et seulement si $N(z) = 1$. En déduire quels sont les éléments inversibles de $\mathbb{Z}[i]$.
4) Soient $z, z' \in \mathbb{Z}[i]$, avec $z' \neq 0$. Montrer qu'il existe $q, r \in \mathbb{Z}[i]$, avec $N(r) < N(z')$, tels que $z = qz' + r$.
5) En déduire que $\mathbb{Z}[i]$ est principal (*i.e.* tout idéal de $\mathbb{Z}[i]$ est de la forme $z\mathbb{Z}[i]$ pour un $z \in \mathbb{Z}[i]$ convenable).
6) Soit $z \in \mathbb{Z}[i]$ irréductible. Montrer que l'idéal $z\mathbb{Z}[i]$ est maximal (on rappelle qu'un élément x d'un anneau intègre A est dit *irréductible* si x n'est pas inversible, et si lorsque $x = ab$ avec $a, b \in A$, alors a ou b est inversible ; un élément réductible est un élément qui n'est ni inversible, ni irréductible).

On fixe maintenant un nombre premier $p \in \mathbb{N}$.
7) Montrer que p est réductible dans $\mathbb{Z}[i]$ si et seulement si p s'écrit sous la forme $p = a^2 + b^2$, avec $a, b \in \mathbb{Z}$.
On suppose que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire qu'il existe un entier $a \in \mathbb{Z}$ tel que $a^2 \equiv -1 \pmod{p}$. On veut montrer que p est réductible dans $\mathbb{Z}[i]$.
9) Monter que si p est irréductible, il existe $a \in \mathbb{Z}$ tel que p divise $a - i$ et $a + i$ (on pourra utiliser la question 6.). En déduire que p divise a, et en tirer une contradiction.
10) On suppose que p est réductible dans $\mathbb{Z}[i]$. En écrivant $p = a^2 + b^2$ et en remarquant que p ne peut pas diviser b, montrer que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.