122 – Anneaux principaux. Applications.

2013 – 2014

Question.

Soit A principal. Quel est le lien entre les idéaux premiers et les idéaux maximaux de A ?

Réponse.

Les idéaux maximaux sont premiers. $\{0\}$ est premier car $A/\{0\} \simeq A$ est intègre mais $\{0\}$ n'est maximal que si A est un corps.

Montrons que tous les autres idéaux premiers de A sont maximaux. Soit $I \neq \{0\}$ un idéal premier, alors il existe $a \in A$ tel que $I = (a)$ car A est principal. Soit J un idéal de A tel que $I \subset J$, alors il existe $b \in A$ tel que $J = (b)$, on a donc $b \mid a$, c'est-à-dire $a = bc$ pour un certain $c \in A$. On a donc $bc \in I$ donc $b \in I$ ou $c \in I$ car I est premier.

Si $b \in I$, alors $I = J$. Sinon, $c \in I$ donc $a \mid c$ et $c \mid a$, donc il existe $k \in A^\times$ tel que $c = ka = kbc$. On en déduit $c(1 - kb) = 0$, d'où $c = 0$ ou $kb = 1$. Si $c = 0$, alors $a = 0$, ce qui est exclu. Donc $kb = 1$ et donc $b \in A^\times$, donc $J = A$.

Question.

Soit A un anneau commutatif unitaire. Montrer que $A[X]$ est euclidien si et seulement si A est un corps.

Réponse.

Si A est un corps, $A[X]$ est euclidien de jauge le degré (appliquer l'algorithme de division de polynômes).

Si $A[X]$ est euclidien, alors il est principal. Montrons que X est irréductible dans $A[X]$: si $X = PQ$, alors on peut supposer sans perdre en généralité que $\deg P = 1$ et $\deg Q = 0$, c'est-à-dire $X = (aX + b)c = acX + bc$. On en déduit $ac = 1$ et $bc = 0$, c'est-à-dire a et c sont inversibles et $b = 0$ (car c est inversible).

On en déduit que (X) est premier dans $A[X]$, donc maximal car $A[X]$ est principal, donc $A[X]/(X) \simeq A$ est un corps.

Question.

Donner un anneau non principal dans lequel les idéaux premiers non nuls sont maximaux.

Réponse.

On considère $A := \mathbb{Z}[i\sqrt{5}]$. Montrons que A n'est pas factoriel (donc non principal).

On a $6 = 2 \times 3 = (1+i\sqrt{5})(1-i\sqrt{5})$. On introduit alors l'application $N : z \mapsto z\bar{z}$ sur A et on a $a \in A^\times$ si et seulement si $N(z) = 1$. En effet, si $N(z) = 1$ alors $z\bar{z} = 1$ donc z est inversible, si $zz' = 1$, alors $N(zz') = N(z)N(z') = 1$ et $N(z) \in \mathbb{N}$ donc $N(z) = 1$. Donc les éléments $2, 3, 1+i\sqrt{5}$ et $1-i\sqrt{5}$ ne sont pas inversibles. Montrons par ailleurs que ces éléments sont irréductibles.

Pour $z = a + ib\sqrt{5} \in A, N(z) = a^2 + 5b^2$ donc $N(z)$ est un carré modulo 5, donc $N(z) \equiv \pm 1[5]$. Maintenant, si z n'est pas irréductible, $z = xy$ avec x et y non inversibles donc $N(z) = N(x)N(y)$ avec $N(x), N(y) \neq 1$ (car x et y sont non inversibles) et $N(x), N(y) \equiv \pm 1[5]$. Or $N(2) = 4, N(3) = 9, N(1+i\sqrt{5}) = N(1-i\sqrt{5}) = 6$ et on vérifie à chaque fois qu'une telle écriture n'est pas possible $(4 = 2 \times 2, 9 = 3 \times 3, 6 = 3 \times 2)$.

Il s'agit maintenant de montrer que si I est un idéal premier non nul, alors A/I est un corps. A/I est intègre, il suffit donc de montrer que A/I est fini (un anneau unitaire intègre fini est un corps). A est un $\mathbb{Z}$-module libre de rang 2 (dont une base est $(1, i\sqrt{5})$) et I est un sous-$\mathbb{Z}$-module de A, donc d'après le théorème de la base adaptée il existe une base (e_1, e_2) de A et $d_1, d_2 \in \mathbb{Z}$ tels que (d_1e_1, d_2e_2) soit une famille génératrice de I. De plus, les d_i sont non nuls car I contient le sous-$\mathbb{Z}$-module de rang 2 αA pour $\alpha \in I \setminus \{0\}$, donc (d_1e_1, d_2e_2) est une base de I et on a $A/I \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z})$, qui est fini.