Correction de l'exercice 3, TD 5

Exercice 3

1. Si $xy \in I \cap \mathbb{Z}$, alors $xy \in I$ supposé premier. Donc x ou y est dans I, et x ou y est dans $I \cap \mathbb{Z}$. C'est donc un idéal premier de $\mathbb{Z}$.
2. Supposons que $I \cap \mathbb{Z} = \{0\}$.
   Premièrement, montrons que si $P \in I$, alors $\frac{P}{c(P)} \in I$, où $c(P)$ est le contenu de P. Supposons par l'absurde que ce n'est pas le cas. Alors modulo I, $\overline{c(P)} \neq 0$ car $\mathbb{Z} \cap I = \{0\}$, et $\overline{(\frac{P}{c(P)})} \neq 0$, et

   $$\overline{0} = \overline{P} = \overline{c(P)} \times \overline{\left(\frac{P}{c(P)}\right)} \neq 0$$

   par intégrité de $\mathbb{Z}[X]/I$ (car I premier). C'est absurde.
   Montrons que $I = \tilde{I} \cap \mathbb{Z}[X]$, où $\tilde{I} = I\mathbb{Q}[X]$. Il est clair que $I = I\mathbb{Z}[X] \subset \tilde{I}$, et donc $I \subset \tilde{I} \cap \mathbb{Z}[X]$. Montrons l'inclusion réciproque. Soit $P \in \tilde{I} \cap \mathbb{Z}[X]$. Il existe $P_0 \in I$ et $A \in \mathbb{Q}[X]$ tels que $P = P_0 \times A$. En écrivant $P_0 \times A = \frac{P_0}{c(P_0)} \times c(P_0)A$, on peut supposer P_0 primitif (et toujours dans I par la remarque précédente). Soit $q = \min\{n > 0, nA \in \mathbb{Z}[X]\}$. Alors $qP = P_0 \times qA$. Par le lemme de Gauss, $q \times c(P) = c(P_0) \times c(qA) = c(qA)$. Donc q divise le contenu de qA, et $A = \frac{1}{q}(qA) \in \mathbb{Z}[X]$. Il vient que $P = P_0 \times A$ avec $P_0 \in I$ et $A \in \mathbb{Z}[X]$, donc $P \in I$. La seconde inclusion est donc vérifiée.
   Montrons enfin que I est principal. Puisque $\mathbb{Q}$ est un corps, $\mathbb{Q}[X]$ est principal, et donc $\tilde{I} = (P_1)$. Quitte à multiplier par le ppcm des dénominateurs des coefficients (sous forme irréductible) de P_1, on peut supposer $P_1 \in \mathbb{Z}[X]$ entier, et quitte à le diviser par son contenu, on peut le supposer primitif. Montrons alors que $I = (P_1)$ dans $\mathbb{Z}[X]$. Il est clair que $(P_1) \subset I$. Réciproquement, si $P \in I$, l'étude précédente montre que $P = P_1 \times A$ dans $\mathbb{Q}[X]$, avec A à coefficients entiers, donc $P = P_1 \times A$ dans $\mathbb{Z}[X]$, et la réciproque est vérifiée.
   Finalement, $I = (P)$ avec P primitif. Puisque I est premier, P est irréductible.

3. Supposons $I \cap \mathbb{Z} = p\mathbb{Z}$ avec p premier. Considérons le morphisme naturel $\phi\colon \mathbb{Z}[X] \to \mathbb{F}_p[X]$ de réduction modulo p.
   (a) Si $\phi(I) = \{0\}$, alors $I \subset (p)$ et $I = (p)$.
   (b) Si $\phi(I) \neq \{0\}$, alors il existe un polynôme non nul unitaire $\overline{P_0} \in \mathbb{F}_p[X]$ tel que $\phi(I) = (\overline{P_0})$ (car $\mathbb{F}_p$ est un corps, donc $\mathbb{F}_p[X]$ est principal). On peut de plus choisir $\overline{P_0}$ unitaire, et par conséquent un relevé $P_0 \in \mathbb{Z}[X]$ unitaire. Puisque I est premier et ϕ est surjective, $\phi(I)$ est premier, et $\overline{P_0}$ est irréductible dans $\mathbb{F}_p[X]$.
   Montrons que $I = (p, P_0)$. L'inclusion $(p, P_0) \subset I$ est claire. Réciproquement, si $P \in I$ alors $\phi(P) \in \phi(I) = (\overline{P_0})$, est il existe A, B tels que $P = P_0 \times A + pB$.
4. On a montré que les idéaux premiers de $\mathbb{Z}[X]$ sont de la forme :
   — $\{0\}$,
   — $(P(X))$ avec $P(X)$ irréductible primitif,
   — (p) avec p premier,
   — $(p, P(X))$ avec p premier et $P(X)$ unitaire irréductible modulo p.
   Comme $\mathbb{Z}[X]/\{0\} \simeq \mathbb{Z}[X]$ et $\mathbb{Z}[X]/(p) \simeq \mathbb{F}_p[X]$ ne sont pas des corps, $\{0\}$ et (p) ne sont pas maximaux. Montrons que si P est irréductible primitif, alors (P) n'est pas maximal. Soit $m \in \mathbb{Z}$ tels que $P(m) \notin \{-1, 0, 1\}$, ce qui est possible car P n'est pas constant, et soit p un diviseur premier de $P(m)$. Montrons que $(P) \subsetneq (p, P) \subsetneq \mathbb{Z}[X]$. La première inclusion est triviale. Supposons par l'absurde que $(p, P) = \mathbb{Z}[X]$. Alors il existe A et B dans $\mathbb{Z}[X]$ tels que $1 = A(X) \times p + B(X) \times P(x)$. En évaluant en m, on a $1 = A(m) \times p$, ce qui est absurde. Ainsi, (P) n'est pas maximal.
   Finalement, seuls les idéaux de la forme $(p, P) = (p) + (P)$, avec P unitaire irréductible modulo p, peuvent être maximaux. Notons toujours ϕ le morphisme de réduction modulo p. Remarquons que
   $$\mathbb{Z}[X]/(p, P) \simeq (\mathbb{Z}/(p))/((p, P)/(p)) \simeq \mathbb{F}_p[X]/\phi(P)$$
   qui est un corps puisque $\phi(P)$ est irréductible dans $\mathbb{F}_p[X]$ principal. Ainsi, (p, P) est maximal.
5. Il s'agit d'appliquer la même méthode dans $\mathbb{C}[X, Y] = (\mathbb{C}[X])[Y]$: tout fonctionne pareil, car $\mathbb{C}[X]$ est principal. On obtient que les idéaux premiers sont de la forme :
   — $\{0\}$,
   — $(P(X, Y))$ avec $P(X, Y)$ irréductible primitif, dans $(\mathbb{C}[X])[Y]$, ce qui signifie qu'en écrivant $P(X, Y) = \sum_{i=0}^{n} P_i(X) Y^i$, les polynômes $P_1, \ldots, P_n$ sont premiers entre eux dans leur ensemble dans $\mathbb{C}[X]$,
   — $(P(X))$ avec P irréductible dans $\mathbb{C}[X]$, donc $P(X) = X - a$ pour un certain $a \in \mathbb{C}$,

— $(P(X), Q(X,Y))$ avec $P(X)$ irréductible dans $\mathbb{C}[X]$ (donc $P(X) = X - a$) et $Q(X,Y)$ unitaire, irréductible dans $\mathbb{C}[X,Y]/(P(X)) \simeq \mathbb{C}[Y]$. En particulier, $Q(X,Y) = (X-a)R(X,Y) + Y - b$. Finalement, cet idéal s'écrit $(X-a, Y-b)$.

On montre aisément que seul le dernier cas fournit un idéal maximal.

Remarque : comme corollaire d'un théorème important (*Nullstellensatz* de Hilert), les idéaux maximaux de $k[X_1, \dots, X_n]$, où k est un corps algébriquement clos, sont de la forme $(X_1 - a_1, \dots, X_n - a_n)$.