Corrigé du devoir surveillé

Mercredi 4 mars 2015

Rappel. Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et les $p\mathbb{Z}$ avec p premier.

Exercice 1. 1) Soit I un idéal premier. On a toujours $I \subset r(I)$. Soit $x \in r(I)$: il existe $k \geq 1$ tel que $x^k \in I$. Si $k = 1$, on a $x \in I$. Sinon écrivons $x^k = x^{k-1}x \in I$. Comme I est premier, on a $x \in I$ ou $x^{k-1} \in I$. Une récurrence immédiate sur k sur ce même principe montre que $x \in I$. Donc $I = r(I)$ et l'idéal I est radical.

2) Dans $\mathbb{Z}$, l'idéal $6\mathbb{Z}$ n'est pas premier (car 6 n'est pas premier). Par ailleurs $r(6\mathbb{Z})$ est l'intersection des idéaux premiers de $\mathbb{Z}$ contenant $6\mathbb{Z}$. Or $6\mathbb{Z}$ n'est pas contenu dans $\{0\}$, et $6\mathbb{Z} \subset p\mathbb{Z}$ avec p premier équivaut à $p \mid 6$ c'est-à-dire $p \in \{2, 3\}$. Donc $r(6\mathbb{Z}) = 2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$. L'idéal $6\mathbb{Z}$ est donc radical.

Exercice 2. 1) Soit I un idéal de A. L'application suivante est une bijection :

$$\begin{array}{rcl} \{\text{idéaux de } A \text{ contenant } I\} & \longrightarrow & \{\text{idéaux de } A/I\} \\ J & \longmapsto & J/I = \{j \bmod I \mid j \in J\}. \end{array}$$

Sa réciproque est $K \mapsto \pi^{-1}(K)$ où $\pi : A \to A/I$ désigne la surjection canonique.

2) Par le théorème d'isomorphisme $(A/I)/(J/I) \simeq A/J$, l'idéal J/I est premier si et seulement si A/J est intègre, si et seulement si J est premier. Par restriction, la bijection de la question précédente induit donc une bijection de $V(I)$, qui est l'ensemble des idéaux premiers de A contenant I, sur $\mathrm{Spec}(A/I)$.

3) Par la question précédente, $\mathrm{Spec}(\mathbb{Z}/n\mathbb{Z})$ a même cardinal que

$$V(n\mathbb{Z}) = \{\text{idéaux premiers } \mathfrak{p} \text{ de } \mathbb{Z}, n\mathbb{Z} \subset \mathfrak{p}\}.$$

Comme $n \geq 1$, $n\mathbb{Z}$ n'est pas contenu dans l'idéal $\{0\}$. De plus pour tout premier p, $n\mathbb{Z}$ est contenu dans $p\mathbb{Z}$ si et seulement si p divise n. Donc le cardinal de $V(n\mathbb{Z})$ est le nombre de facteurs premiers distincts de n, ce qui conclut.

Exercice 3. 1) Supposons $B_1 \times B_2$ intègre. La relation $(0, 1)(1, 0) = (0, 0)$ entraîne $(0, 1) = (0, 0)$ ou $(1, 0) = (0, 0)$, c'est-à-dire : $1 = 0$ dans B_2 ou $1 = 0$ dans B_1. Autrement dit, B_1 ou B_2 est l'anneau nul. Supposons par exemple $B_1 = \{0\}$. Si $a, b \in B_2$ vérifient $ab = 0$ alors $(0, a)(0, b) = (0, ab) = (0, 0)$. L'intégrité de $B_1 \times B_2$ entraîne $(0, a) = (0, 0)$ ou $(0, b) = (0, 0)$ donc $a = 0$ ou $b = 0$ dans A_2. Enfin l'anneau B_2 n'est pas nul (car $B_1 \times B_2$ est intègre donc non nul). Cela prouve que B_2 est intègre.

Réciproquement supposons $B_1 = \{0\}$ et B_2 intègre par exemple (on s'y ramène par symétrie du problème). Soient $x = (0, a)$, $y = (0, b)$ éléments quelconques de $B_1 \times B_2$. Supposons $xy = (0, 0)$. Alors on a $(0, 0) = (0, ab)$ d'où $ab = 0$ dans B_2. Par intégrité de B_2, cela entraîne $a = 0$ ou $b = 0$ c'est-à-dire $x = (0, 0)$ ou $y = (0, 0)$. Enfin l'anneau $B_1 \times B_2$ n'est pas nul car $B_2 \neq \{0\}$ (puisque B_2 est intègre). Donc l'anneau $B_1 \times B_2$ est intègre.

2) (a) Soit $J = I_1 \times I_2$ où I_1 (resp. I_2) est un idéal de A_1 (resp. A_2). En utilisant la question 1), on obtient l'équivalence des affirmations suivantes :
- l'idéal J est premier ;
- l'anneau $A/J = (A_1/I_1) \times (A_2/I_2)$ est intègre (cette écriture de A/J est possible car les lois sur $A_1 \times A_2$ s'effectuent composante par composante) ;

- ($A_1/I_1 = \{0\}$ et A_2/I_2 est intègre) ou (A_1/I_1 est intègre et $A_2/I_2 = \{0\}$)
- ($I_1 = A_1$ et I_2 est premier) ou (I_1 est premier et $I_2 = A_2$).

Cela caractérise les idéaux premiers de A et se traduit en la partition $\operatorname{Spec} A = S_1 \sqcup S_2$ où $S_1 = \{\mathfrak{p} \times A_2 \mid \mathfrak{p} \in \operatorname{Spec} A_1\}$ et $S_2 = \{A_1 \times \mathfrak{q} \mid \mathfrak{q} \in \operatorname{Spec} A_2\}$ (en effet les ensembles S_1 et S_2 sont disjoints car tout idéal premier $\mathfrak{p}$ de A_1 est propre, par définition).

(b) La topologie de Zariski sur un anneau quelconque B est définie en décidant que ses ensembles fermés sont les $V(E) = \{\mathfrak{p} \in \operatorname{Spec} B \mid E \subset \mathfrak{p}\}$ où E parcourt l'ensemble des parties de B.

(c) Pour montrer que l'espace topologique $\operatorname{Spec} A$ n'est pas connexe, il suffit de voir que S_1 et S_2 sont des fermés (on sait déjà qu'ils sont disjoints). En comparant S_1 à S_2, on voit que S_1 coïncide avec l'ensemble des idéaux premiers de A contenant $(0,1)$ (cela utilise le fait que tout idéal premier est propre). Ainsi on a $S_1 = V((0,1))$. De même on obtient $S_2 = V((1,0))$. Les ensembles S_1 et S_2 sont fermés non vides et disjoints donc $\operatorname{Spec} A$ n'est pas connexe.

Exercice 4. Fixons un entier $n \geq 1$ et un corps **algébriquement clos** K. Soit A la K-algèbre $K[X_1, \dots, X_n]$.

1) Soit T une partie de A. On a $T \subset I_T$ donc $Z(I_T) \subset Z(T)$. Montrons l'inclusion inverse. Soit $\alpha \in Z(T)$. Tout polynôme de I_T s'écrit $P = \displaystyle\sum_{k=1}^{n} A_k T_k$ avec $n \geq 1$, $A_k \in A$ et $T_k \in T$. Or $T_k(\alpha)$ est nul pour tout k donc $P(\alpha) = 0$. Cela montre que $\alpha \in Z(I_T)$ et $Z(I_T) = Z(T)$.

2) Soit Y une partie de K^n. L'ensemble $\mathcal{I}(Y)$ est non vide car il contient 0. Pour tous $P, Q \in \mathcal{I}(Y)$ et $R \in A$, et pour tout $\alpha \in Y$, on a

$$(P - Q)(\alpha) = P(\alpha) - Q(\alpha) = 0 - 0 = 0$$
$$(RP)(\alpha) = R(\alpha)P(\alpha) = R(\alpha) \times 0 = 0.$$

Donc $P - Q$ et RP appartiennent à $\mathcal{I}(Y)$. Ainsi $\mathcal{I}(Y)$ est un idéal de A.

3) Supposons $Y = Y_1 \cup Y_2$. Un polynôme appartient à $\mathcal{I}(Y)$ si et seulement s'il s'annule sur $Y_1 \cup Y_2$ c'est-à-dire s'il s'annule sur Y_1 et sur Y_2. Autrement dit on a $\mathcal{I}(Y) = \mathcal{I}(Y_1) \cap \mathcal{I}(Y_2)$.

4) Soit I un idéal de A tel que $Z(I)$ est fini non vide. On note $Z(I) = \{\alpha_1, \dots, \alpha_t\}$ où $\alpha_1, \dots, \alpha_t$ sont des éléments de K^n.

(a) Sur le corps algébriquement clos K, le théorème des zéros affirme que

$$r(I) = \mathcal{I}(Z(I)) = I(\alpha_1, \dots, \alpha_t).$$

En utilisant la question 3) et en posant $I_j = \mathcal{I}(\alpha_j)$, on obtient $r(I) = I_1 \cap \dots \cap I_t$.

(b) Notons $\alpha_j = (a_{j,1}, \dots, a_{j,n}) \in K^n$. Posons $P_i = \displaystyle\prod_{k=1}^{t} (X_i - a_{k,i})$. Soit $j \in \{1, \dots, t\}$. Comme ce polynôme ne comporte que l'indéterminée X_i, il vérifie

$$P_i(\alpha_j) = P_i(a_{j,i}) = \prod_{k=1}^{t} (a_{j,i} - a_{k,i}) = 0$$

(à cause du terme $k = j$ du produit). Donc P_i appartient à I_j pour tout j, ce qui prouve $P_i \in I_1 \cap \dots \cap I_t$.

(c) Les deux questions précédentes entraînent $P_i \in r(I)$. Il existe donc $m \geq 1$ (dépendant de i) tel que $P_i^m \in I$. Posons $Q_i(X_i) = P_i^m$. C'est un polynôme en l'indéterminée X_i à coefficients en K. De plus, il est de degré $m \deg P_i = mt \geq 1$. Enfin $Q_i(X_i)$ est unitaire car P_i est unitaire.

(d) *Remarque préliminaire.* L'anneau quotient A/I est bien un K-espace vectoriel : c'est le quotient du K-espace vectoriel A par le sous-espace vectoriel I (en effet, l'idéal I est stable par addition, et par multiplication par les scalaires de K).

L'idée générale est de considérer des divisions euclidiennes par les $Q_i(X_i)$, afin d'obtenir des restes de degré $< d_i$ en X_i. L'argument est cependant un peu délicat à écrire.

Soit P quelconque dans A. La division euclidienne généralisée de P par le polynôme unitaire $Q_n(X_n)$ dans $K[X_1, \ldots, X_{n-1}][X_n]$ assure que P est congru modulo I à son reste, un polynôme $R_n \in A$ de degré $k < d_n$ en X_n. Maintenant écrivons

$$R_n = R_{n,0} + R_{n,1}X_n + \cdots + R_{n,k}X_n^k$$

avec $R_{n,0}, \ldots, R_{n,k}$ dans $K[X_1, \ldots, X_{n-1}]$. Chaque division euclidienne de $R_{n,i}$ par $Q_{n-1}(X_{n-1})$ dans $K[X_1, \ldots, X_{n-2}][X_{n-1}]$ fournit un reste dans $K[X_1, \ldots, X_{n-1}]$ de degré $< d_{n-1}$ en X_{n-1}. On en déduit que R_n (donc P) est congru modulo I à un polynôme de degré $< d_n$ en X_n et $< d_{n-1}$ en X_{n-1}. Par une récurrence immédiate [1] sur n, on obtient que P est congru modulo I à un polynôme de degré $< d_i$ en X_i pour tout i. Un tel polynôme est une combinaison K-linéaire de monômes $X_1^{m_1} \cdots X_n^{m_n}$ avec pour tout i, $0 \leq m_i < d_i$. La famille $\{X_1^{m_1} \cdots X_n^{m_n} \bmod I \mid \forall i, 0 \leq m_i < d_i\}$ engendre donc A/I comme K-espace vectoriel. Cette famille étant finie, cet espace vectoriel est de dimension finie sur K.

5) Soit I un idéal de A tel que $Z(I)$ est vide. Le théorème des zéros dans sa version faible sur le corps algébriquement clos K dit alors que $I = A$. En particulier $A/I = \{0\}$, qui est de dimension nulle comme K-espace vectoriel.

Commentaire. Cet exercice démontre que si $Z(I)$ est fini, alors le K-espace vectoriel A/I est de dimension finie. La réciproque est vraie et se démontrerait avec un peu plus de travail.

Barème :
Exercice 1 : 1) 1,5 pt 2) 1 pt
Exercice 2 : 1 pt par question
Exercice 3 : 1) 2 pts 2a) 1,5 pt 2b) 1 pt 2c) 1 pt
Exercice 4 : 1) 1 pt 2) 1 pt 3) 1 pt 4a) 1 pt 4b) 0,5 pt 4c) 1 pt 4d) 2,5 pts 5) 1 pt.

1. Une rédaction rigoureuse consisterait à écrire cette récurrence.