Exercices Algèbre - Anneaux II

Tous les anneaux de cette feuille d'exercices sont supposés être commutatif sauf mention explicite du contraire.

Exercice 1. Montrer qu'un polynôme $P(X,Y) \in \mathbb{Z}[X,Y]$ est tel que $P(T^2,T^3) = 0$ si, et seulement si, il existe un polynôme $Q(X,Y) \in \mathbb{Z}[X,Y]$ tel que $P(X,Y) = (X^3 - Y^2) \cdot Q(X,Y)$.

Solution. Le sens indirect est clair. Écrivons $\mathbb{Z}[X,Y] = A_X[X][Y]$ où $A_X = \mathbb{Z}[X]$. On divise $P \in A_X[Y]$ par le polynôme unitaire $(X^3 - Y^2) \in A_X[Y]$ vu comme des polynôme en Y : il existe $Q(X,Y)$ et $R_X(Y) \in A_X[Y]$ avec $P(X,Y) = (X^3 - Y^3)Q(X,Y) + R_X(Y)$ et $\deg_Y R_X(Y) < 2$; donc $R_X(Y) = AY + B$ où $A, B \in \mathbb{Z}[X]$. Donc, si $P(T^2,T^3) = 0$ alors $A(T^2)T^3 + B(T^2) = 0$. Le degré de $A(T^2)T^3$ comme polynôme de T étant de la forme $2k+3$ et celui de $B(T^2)$ étant de la forme $2l$ pour $k, l \in \mathbb{N}$, on obtient que $A = B = 0$.

Exercice 2. Soit k un corps et N un entier naturel. On considère l'anneau de polynômes $A := k[X_1, \ldots, X_N]$, un élément $a = (a_1, \ldots, a_N)$ de k^N et un élément P de A.
Vérifier que l'on définit des idéaux de A en posant

$$I_1 := (P) = P.A$$

et

$$I_2 := \{Q \in k[X_1, \ldots, X_N] \mid Q(a) = 0\}.$$

Montrer que I_1 et I_2 sont des idéaux étrangers si et seulement si $P(a) \neq 0$. (Par définition, I_1 et I_2 sont des idéaux étrangers de A si $I_1 + I_2 = A$)

Solution. Si I_1 et I_2 sont étrangers, il existe $Q_1 \in I_1$ et $Q_1 \in I_2$ tels que $1 = Q_1 + Q_2$, donc, il existe $Q_1' \in A$ et $Q_2 \in I_2$ tels que $1 = Q_1'(X)P(X) + Q_2(X)$, en particulier, $1 = Q_1(a)P(a) + Q_2(a)$, comme $Q_2(a) = 0$ on a forcément que $P(a) \neq 0$.
Réciproquement, si $P(a) \neq 0$ alors $P(a)$ est inversible et on peut écrire $1 = P(a)^{-1}P + (1 - P(a)^{-1}P)$; on remarque que $P(a)^{-1}P \in I_1$ et $(1 - P(a)^{-1}P) \in I_2$ donc I_1 et I_2 sont étrangers.

Exercice 3. Un anneau commutatif est dit *local* s'il n'admet qu'un seul idéal maximal.

1. Montrer qu'un anneau commutatif est local si, et seulement si, l'ensemble de ses éléments non inversibles est un idéal, et que dans ce cas, cet idéal est l'unique idéal maximal.
2. Montrer qu'un anneau commutatif est local si, et seulement si, pour tout élément x de cet anneau, au moins l'un de x ou $1 - x$ est inversible.
3. Un élément x est dit *idempotent* si $x^2 = x$. Montrer que si A est un anneau local, alors ses seuls idempotents sont 1 et 0. Donner un exemple d'anneau pour lequel la réciproque est fausse.
4. Soient k un corps et n un entier strictement positif. Montrer que $k[x]/(x^n)$ est un anneau local, et déterminer son idéal maximal.
5. Soit p un nombre premier, et soit $\mathbb{Z}_{(p)}$ la localisation de $\mathbb{Z}$ par rapport à l'idéal premier (p). Montrer que $\mathbb{Z}_{(p)}$ est local, et calculer son idéal maximal.
6. L'ensemble des *germes de fonctions continues en* 0 est l'ensemble des classes d'équivalence de couples (f, U), où U est un intervalle ouvert de $\mathbb{R}$ contenant 0 et $f : U \to \mathbb{R}$ est une fonction continue, pour la relation d'équivalence définie par : $(f, U) \sim (g, V)$ si, et seulement si, il existe un ouvert W non vide contenu dans $U \cap V$ tel que $f|_W = g|_W$.
   Montrer que cet ensemble, muni de la somme et du produit induits par ceux pour les fonctions continues, est un anneau commutatif local.

SOLUTION.

1. Notons $I = \{x \in A \mid x \notin A^\times\}$. Supposons que c'est un idéal. Soit J un idéal de A. Alors pour tout $y \in J$, $y \notin A^\times$ car sinon $J = A$, donc $J \subset I$ et I est alors maximal et c'est le seul car il contient tous les autres idéaux de A qui est donc local.
   Réciproquement, supposons A local et montrons que I est un idéal. Soit M l'idéal maximal de A, il est contenu dans I car tous les éléments de M sont non inversibles. Soient $x, y \in I$ et montrons que $x - y \in I$. Come M est le seul idéal maximal de A on a que l'idéal engendré par $x - y$ est contenu dans M qui est contenu dan s I donc $x - y \in I$. Comme I est non vide car $0 \in I$ on a bien que $(I, +)$ est un sous-groupe de $(A, +)$. En plus, si $x \in I$, on a que l'idéal engendré par x est forcément contenu dans M, donc pour tout $a \in A$, $ax \in M \subset I$.
2. Supposons A local et supposons $x \notin A^\times$; alors $x \in I = A\backslash A^\times$ qui est un idéal. Si $1 - X \in I$, alors $1 = 1 - x + x \in I$ mais $1 \in A^\times$; donc $1 - x \notin I$ et donc $1 - x \in A^\times$. De même, si $1 - x \notin A^\times$ alors $1 - x \in I$ et si $x \in I$ alors $1 \in I$, donc $x \notin I$ et $x \in A^\times$.
   Réciproquement, supposons pour tout $x \in A$, $x \in A^\times$ ou $1 - x \in A^\times$. Soit M un idéal maximal de A et soit $y \in A\backslash M$ alors $(y, M) = A$ et il existe $a \in A$, $m \in M$ tels que $1 = ay + m$ donc $ay = 1 - m \in A^\times$ car $m \in M \neq A$ donc $m \in A^\times$. On a donc montré que (y) contenait un élément inversible, donc $(y) = A$. On a alors que $y \in A^\times$. On a montré que $A\backslash M = A^\times$ donc $A\backslash A^\times = M$ est un idéal et donc A est local.
3. Soit $x \in A$ tel que $x^2 = x$, alors $x^2 - x = x(x - 1) = 0$ et x et $x - 1$ sont des diviseurs de zéro. Comme A est local on a que : soit $x \in A \in A^\times$ et dans ce cas $x = 1$, soit $x - 1 \in A^\times$ et dans ce cas $x = 0$.
   Si $A = \mathbb{Z}$ alors il est intègre donc si $x^2 = x$ on a que $x = 1$ ou $x = 0$, donc les seuls idempotents sont 1 et 0 mais $\mathbb{Z}$ n'est pas local car pour tout nombre premier p, l'idéal $p\mathbb{Z}$ est maximal.
4. Les idéaux de $k[x]/(x^n)$ sont en bijection avec les idéaux de $k[x]$ qui contiennent (x^n) ; comme $k[x]$ est principal, ils sont engendrés par un $P \in k[x]$ tel que $(x^n) \subset (P)$, c'est-à-dire tels que P divise (x^n), ce qui implique que $P = x^k$ avec $k \leq n$. Le seul idéal maximal est alors (x) car pour tout $k \leq n - 1$, on a
   $$(x^n) \subset (x^{n-1}) \subset \cdots \subset (x^k) \subset \cdots \subset (x)$$
5. Pour rappel, $\mathbb{Z}_{(p)} = S^{-1}\mathbb{Z}$ où $S = A\backslash(p)$ qui est une partie multiplicative de $\mathbb{Z}$. On a déjà montré que l'idéal engendré par l'image de (p) était le seul idéal maximal de $\mathbb{Z}_{(p)}$ (cf. feuille 3 exercice 2, question 7.)
6. On vérifie facilement que $G = \{(f, U)\}/\sim$ l'ensemble des germes de fonctions continues en zéro est un anneau pour $(f, U) + (g, V) = (f + g, U \cap V)$, $(f, U).(g, V) = (f.g, U \cap V)$ (l'élément neutre pour + est la fonction nulle définie sur n'importe quel ouvert U, elles sont toutes équivalentes, l'identité est la fonction identité sur $\mathbb{R}$ définie partout.
   Si $f(0) \neq 0$ alors f est inversible au voisinage de 0 donc sa classe est inversible dans G. Si $f(0) = 0$ alors $(1 - f)(0) \neq 0$ et donc est inversible au voisinage de 0, sa classe est donc inversible dans G, qui est alors local.

EXERCICE 4. Soit $Q \in \mathbb{Z}[X]$ unitaire. On note $z_1, ..., z_n$ ses racines (pas forcément distinctes) dans $\mathbb{C}$. Montrer que
$$\prod_{i \neq j} (z_i - z_j) \in \mathbb{Z}.$$

SOLUTION. On observe que le polynôme en n indéterminées
$$P = \prod_{i \neq j} (X_i - X_j)$$

est un polynôme symétrique de $\mathbb{Z}[X_1, ..., X_n]$; en effet, il est clairement invariant pour l'action de toute transposition, et les transpositions engendrent $\mathcal{S}_n$. D'après le théorème de structure, il existe $R \in \mathbb{Z}[X_1, ..., X_n]$ tel que

$$P = R(\sigma_1, ..., \sigma_n),$$

où les σ_i sont les polynômes symétriques élèmentaires. D'autre part, on a

$$Q = \prod_{i=1}^{n}(z - z_i) = z^n - \sigma_1(z_1, ..., z_n)z^{n-1} + ... + (-1)^n\sigma_n(z_1, ..., z_n),$$

ce qui montre que chaque $\sigma_i(z_1, ..., z_n)$ est entier. Du coup,

$$P(z_1, ..., z_n) = R(\sigma_1(z_1, ..., z_n), ..., \sigma_n(z_1, ..., z_n))$$

est bien entier comme on voulait.

EXERCICE 5. 1. Calculer $A[X]^\times$ lorsque A est un anneau quelconque.

2. Soit B un anneau et A un sous-anneau de B. Soit $b \in B$. On dit que b est *entier* sur A s'il vérifie une équation unitaire :

$$b^n + a_{n-1}b^{n-1} + ... + a_0 = 0 \quad \text{avec} \quad a_0, ..., a_{n-1} \in A.$$

Un anneau intègre est dit *intégralement clos* si pour tout $x \in K = \mathrm{Frac}(A)$, si x est entier sur A alors $x \in A$.

(a) Montrer qu'un anneau factoriel est intégralement clos.

(b) Soit $d \in \mathbb{Z}$ un entier sans facteur carré non nul. On pose :

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

Montrer que si $d \equiv 1 \pmod 4$, alors $\mathbb{Z}[\sqrt{d}]$ n'est pas intégralement clos (considérer l'élément $\frac{1+\sqrt{d}}{2}$).

SOLUTION.

1. On peut montrer que $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]^\times$ si et seulement si $a_0 \in A^\times$ et $a_1, \ldots, a_n$ spnt nilpotents.

2. (a) Soit $x \in K = \mathrm{Frac}(A)$ un élément entier sur A. Comme A est factoriel il existe $p, q \in A$ premier entre eux tels que $x = \frac{p}{q}$; x étant entier sur A il existe $a_0, \ldots, a_{n-1} \in A$ tels que

$$(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0$$

donc $p^n = -a_{n-1}p^{n-1}q - \cdots - a_1pq^{n-1} - a_0q^n$, comme q divise le membre de droite on a que q divise p^n, or on a supposé que p et q étaient premiers entre eux et comme A est factoriel par le lemme de Gauss, on a que q divise 1 et donc q est inversible dans A. On a alors que $x = pq^{-1} \in A$.

(b) Considérons $\alpha = \frac{1+\sqrt{d}}{2}$. Alors $\alpha^2 - \alpha - \frac{d-1}{4} = 0$. Comme $d \equiv 1[4]$, on a que α est bien entier donc $\mathbb{Z}[\sqrt{d}]$ n'est pas intégralement clos.

EXERCICE 6. Soit K un corps. Soit $A = K[X, Y]$. On note B la sous-algèbre de A engendrée par les XY^n pour $n \in \mathbb{N}$.

1. Montrer que si $Q(X, Y)$ est dans B, alors $Q(0, Y)$ est un polynôme constant.
2. Soit $r \in \mathbb{N}^*$. Comparer les idéaux de B engendrés par $(X, XY, ..., XY^r)$ et $(X, XY, ..., XY^r, XY^{r+1})$.
3. La K-algèbre B est-elle un anneau noethérien ? Une K-algèbre de type fini ?

SOLUTION.

1. Pour tout monôme non constant
$$S = \lambda X_0^{\alpha_0} X_1^{\alpha_1} ... X_r^{\alpha_r} \in K[X_0, ..., X_r]$$
(avec $\lambda \in K$), on a $R := S(X, XY, ..., XY^r)$ divisible par X dans $K[X, Y]$, ce qui implique que $R(0, Y) = 0$. Comme un élèment Q de B est un polynôme à coefficients dans K en les XY^n, c'est la somme d'une constante et d'une somme de polynômes R comme ci-dessus, d'où le résultat.
2. Clairement, l'idéal $I := (X, XY, ..., XY^r)$ est inclus dans l'idéal $J := (X, XY, ..., XY^r, XY^{r+1})$. Montrons que l'inclusion est stricte en vérifiant que $XY^{r+1} \notin I$. Sinon, on pourrait écrire
$$XY^{r+1} = P_0 X + ... + P_r XY^r,$$
où les P_i sont dans B. Comme l'anneau $B \subset K[X, Y]$ est intègre, on aurait
$$Y^{r+1} = P_0 + ... + P_r Y^r.$$
En faisant $X = 0$ et en appliquant a), on aurait des élèments $\lambda_0, ..., \lambda_r$ de K tels que
$$Y^{r+1} = \lambda_0 + ... + \lambda_r Y^r,$$
ce qui est une contradiction pour raison de degré.
3. Le 2. donne une suite strictement croissante d'idéaux de B, qui n'est donc pas un anneau noethérien, et a fortiori pas une K-algèbre de type fini. Ainsi, la propriété d'être une K-algèbre de type fini ne se conserve pas par passage à une sous-algèbre.

EXERCICE 7. Soit k un corps. On note $F = k(X)$ le corps des fractions rationnelles.

1. Soient $R_1 = P_1/Q_1, ..., R_s = P_s/Q_s$ des élèments de F, avec $P_i \in k[X]$ et Q_i non nul dans $k[X]$ pour tout i de $[1, s]$. Soit B la sous-k-algèbre de F engendrée par $R_1, ..., R_s$. Montrer qu'il existe un polynôme non nul $G \in k[X]$ tel que $B \subset (k[X])[G^{-1}]$.
2. En déduire que F n'est pas de type fini en tant que k-algèbre.

SOLUTION.

1. Par définition, tout élèment f de B est un polynôme en les R_i, et en particulier $f = P/Q$ avec $P \in k(X)$ et Q de la forme $Q_1^{\alpha_1} ... Q_r^{\alpha_r}$, où les α_i sont dans $\mathbb{N}$. Il suffit alors de prendre $G = Q_1 ... Q_r$.
2. Il suffit de montrer qu'une algèbre B comme ci-dessus ne peut pas être égale à $k(X)$. Or, la fraction rationnelle $1/(G + 1)$ n'est clairement pas dans $(k[X])[G^{-1}]$, sinon on pourrait écrire $1/(G + 1) = H/G^m$ avec $H \in k[X]$ premier à G, ce qui contredit $(G + 1)H = G^m$ vu que $(G + 1)$ est premier à G.

EXERCICE 8. Soient B un anneau, L un sous-anneau de B et A un sous-anneau de L. On suppose que L est un corps, que B est un L-ev de dimension finie, et que B est aussi une A-algèbre de type fini. On se propose de montrer que L est une A-algèbre de type fini. Soient $\alpha_1, ..., \alpha_n$ dans B tels que $B = A[\alpha_1, ..., \alpha_n]$.

1. Soit $\beta_1, ..., \beta_m$ une base de B sur L, avec $\beta_1 = 1$. On écrit

$$\beta_i\beta_j = \sum_{k=1}^{m} a_{ijk}\beta_k; \quad \alpha_i = \sum_{j=1}^{m} b_{ij}\beta_j,$$

avec $a_{ijk}, b_{ij} \in L$. Soit C la sous A-algèbre de L engendrée par les a_{ijk} et les b_{ij}. Montrer que tout élément x de B s'écrit :

$$x = \sum_{i=1}^{m} \lambda_i\beta_i,$$

où les λ_i sont dans C.

2. En déduire que $L = C$, et conclure.

SOLUTION.

1. Le plus difficile consiste à digérer les notations... Soit B' l'ensemble des élèments de B de la forme $\sum_{i=1}^{m} \lambda_i\beta_i$ avec les λ_i dans C (c'est le C-module engendré par les β_i). Si x est dans B, c'est un polynôme en les α_i à coefficients dans A. Il suffit donc de montrer que tous les monômes

$$\alpha_1^{r_1}...\alpha_n^{r_n}$$

en les α_i sont dans B'. Comme chaque α_i est une combinaison linéaire des β_j à coefficients dans C, il suffit de montrer que tout monôme

$$\beta_1^{s_1}...\beta_m^{s_m}$$

en les β_j est dans B'. Or, d'aprés la définition des a_{ijk}, chaque β_i (rappelons que $\beta_1 = 1$) et chaque produit $\beta_i\beta_j$ sont dans B'. Ainsi B' est stable par multiplication par chaque β_i, ce qui montre que tous les monômes $\beta_1^{s_1}...\beta_m^{s_m}$ comme ci-dessus sont bien dans B'. Finalement $B' = B$.

2. Soit $y \in L$, alors $y = y\beta_1 \in B$, et d'aprés a) on peut écrire $y = \sum_{i=1}^{m} \lambda_i\beta_i$ avec les λ_i dans $C \subset L$. Mais par unicité de la décomposition d'un élément de B sur la base $(\beta_1, ..., \beta_m)$ du L-ev B, on obtient $y \in C$. Finalement $L = C$, et L est bien de type fini comme A-algèbre.

EXERCICE 9. Cet exercice utilise les exercices 7 et 8. Soient $k \subset K$ deux corps, tels que K soit une k-algèbre de type fini. Le but de l'exercice est de montrer que K est un k-ev de dimension finie. Pour cela on écrit $K = k[\alpha_1, ..., \alpha_n]$, et on raisonne par récurrence en supposant le résultat vrai jusqu'à $n - 1$, le cas $n = 0$ étant trivial.

1. On pose $L = k(\alpha_1)$ (c'est le corps des fractions de $k[\alpha_1]$). Comparer K et $L[\alpha_2, ..., \alpha_n]$, et en déduire que K est de dimension finie sur L.
2. En utilisant l'exercice 8, montrer que L est une k-algèbre de type fini.
3. En utilisant l'exercice 7, montrer que α_1 est racine d'un polynôme unitaire de $k[X]$, puis que L est de dimension finie sur k.
4. En déduire le résultat annoncé (lemme de Zariski).

SOLUTION.

1. Comme K est un corps, il contient $k(\alpha_1)$, et donc aussi $L[\alpha_2, ..., \alpha_n]$. Comme par hypothèse $K = k[\alpha_1, ..., \alpha_n]$, on a finalement $K = L[\alpha_2, ..., \alpha_n]$, et l'hypothèse de récurrence donne alors que K (qui est donc une L-algèbre de type fini) est un L-ev de dimension finie.
2. Il suffit d'appliquer le résultat de
l'exercice 8 avec $A = k$, $L = L$ et $B = K$.

3. Si α_1 n'est pas racine d'un polynôme non nul de $k[X]$, alors le morphisme de k-algèbre de $k[X]$ dans $k[\alpha_1]$ qui envoie X sur α_1 est injectif, donc $k[\alpha_1]$ est isomorphe à $k[X]$ et son corps des fractions L à $k(X)$. Ceci est impossible d'après l'exercice 7 puisque d'après 2., L est une k-algèbre de type fini. Si P est un polynôme unitaire de degré d qui annule α_1, on a alors que $k[\alpha_1] = k(\alpha_1) = \mathrm{Vect}_k(1, \alpha_1, ..., \alpha_1^{d-1})$ est de dimension finie sur k.
4. D'après 3., L est de dimension finie sur k et d'après 1., K est de dimension finie sur L. Donc, K est de dimension finie sur k.

EXERCICE 10. Cet exercice utilise le résultat de l'exercice 9. Soit k un corps.

1. Soient $a_1, ..., a_n$ dans k. Montrer que le morphisme $u : P \mapsto P(a_1, ..., a_n)$ de $k[X_1, ..., X_n]$ dans k est surjectif de noyau l'idéal J engendré par les polynômes $(X_1 - a_1), ..., (X_r - a_r)$.

   On suppose dans la suite que k est algébriquement clos.
2. Soit I un idéal maximal de $k[X_1, ..., X_n]$. Montrer que le corps $L = k[X_1, ..., X_n]/I$ est isomorphe (en tant que k-algèbre) à k (on appliquera le résultat principal de l'exercice 9).
3. En déduire qu'il existe $a_1, ..., a_n$ dans k tel que I soit l'idéal J du a), c'est-à-dire que I est l'ensemble des polynômes $P \in k[X_1, ..., X_n]$ tels que $P(a_1, ..., a_n) = 0$ (théorème des zéros de Hilbert).

SOLUTION.

1. Le morphisme u est surjectif (prendre P constant). Si maintenant $P \in k[X_1, ..., X_n]$, on peut faire la division euclidienne de P par $(X_1 - a_1)$ dans l'anneau $(k[X_1])[X_2, ..., X_n]$, ce qui permet d'écrire $P = Q_1(X_1 - a_1) + R$ avec $R \in k[X_2, ..., X_n]$. Par récurrence, on peut écrire $P = Q_1(X_1 - a_1) + ... + Q_n(X_n - a_n) + b$ avec $b \in k$, après quoi le résultat est évident.
2. Par définition L est une k-algèbre de type fini, donc d'après l'exercice 9 il est de dimension finie sur k. Mais k est algébriquement clos, donc comme tout élément x de L annule un polynôme unitaire à coefficients dans k (vu que $(x^n)_{n\in\mathbb{N}}$ est liée dans le k-ev L), on obtient $x \in k$. Finalement L est isomorphe à k.
3. On vient de voir que le morphisme canonique $k \to k[X_1, ..., X_n]/I$ est un isomorphisme. Soient $a_1, ..., a_n$ les antécédents de $X_1, ..., X_n$, alors par définition les polynômes $(X_i - a_i)$ sont dans I, donc I contient l'idéal J engendré par les $(X_i - a_i)$. Or J est aussi un idéal maximal car d'après a), $k[X_1, ..., X_n]/J$ est un corps (isomorphe à k). Finalement $I = J$.

EXERCICE 11. On rappelle qu'un anneau commutatif A est *noethérien* si, pour toute chaîne d'idéaux

$$I_0 \subset I_1 \subset I_2 \subset \dots$$

de A, il existe un entier N tel que si $n \geq N$, alors $I_n = I_{n+1}$.
Montrer que l'anneau $C^0([0, 1])$ des fonctions continues $[0, 1] \to \mathbb{R}$ n'est pas noethérien. Pour ce faire, on montrera que l'idéal des fonctions s'annulant en 0 n'est pas finiment engendré. (Indication : supposons au contraire qu'il est engendré par $f_1, \dots, f_n$. Alors la fonction $\sqrt{\sum_{i=1}^n |f_i|}$ est une combinaison linéaire des f_i. Montrer que ceci entraîne l'existence d'un M tel que $\sqrt{\sum_{i=1}^n |f_i|} \leq M \sum_{i=1}^n |f_i|$, et que ceci est impossible.)

SOLUTION. On peut montrer plus généralement que l'anneau $A = C^0(X)$ des fonctions continues sur un espace métrique compact X est noethérien si et seulement si X est fini. En effet, soit $x_0 \in X$. Supposons $\{x_0\}$ n'est pas ouvert et pour $n \geq 1$ soit $f_n : x \in X \to d(x, x_0)^{\frac{1}{n!}}$ où d désigne la distance dans X. Si on pose I_n l'idéal engendré par f_n dans A, alors la suite $(I_n)_{n\in\mathbb{N}}$ est une suite croissante d'idéaux de A

qui ne stationne pas. Donc $\{x_0\}$ est forcément ouvert et X est discret. A est donc isomorphe à $\mathbb{R}^X$, les applications de X dans $\mathbb{R}$ qui est noéthérien si X est fini.
Réciproquement, si X est fini alors $A = C(X)$ est isomorphe à $\mathbb{R}^X$ qui est noethérien.

EXERCICE 12. 1. Soit A un anneau factoriel, et soit K un corps des fractions pour A contenant A. Donner un exemple de polynôme réductible dans $A[X]$ et irréductible dans $K[X]$. Donner un exemple de polynôme irréductible dans $A[X]$ et réductible dans $K[X]$.

2. Donner les éléments irréductibles de $\mathbb{Z}[X]$ en fonction de ceux de $\mathbb{Q}[X]$ et de $\mathbb{Z}$.
3. Donner une procédure permettant de déterminer si un polynôme de degré ≤ 3 est irréductible dans $\mathbb{Z}[X]$.
4. Soit K un corps, et soient $P, Q \in K[X]$ premiers entre eux. Montrer que $P \cdot Y + Q$ est irréductible dans $K[X, Y]$.
5. Soit $a \in \mathbb{Z}$. À quelle condition $X^4 - a$ est-il irréductible dans $\mathbb{Q}[X]$? et $X^4 - aX - 1$ dans $\mathbb{Z}[X]$?

SOLUTION.

1. Si P est un polynôme de $A[X]$ irréductible dans $k[X]$ et $a \in A\backslash\{0\}$ non inversible dans A, alors aP est réductible dans $A[X]$ mais irréductible dans $k[X]$ car $a \in k^\times$. Pour trouver un polynôme irréductible dans $A[X]$ mais réductible dans $k[X]$ il suffit de prendre un polynôme irréductible de $A[X]$ qui n'est pas prilitif.
2. Un nombre premier $p\mathbb{Z}$ est irréductible dans $\mathbb{Z}[X]$ comme polynôme de degré 0. Si P est un polynôme irréductible de $\mathbb{Z}[X]$ de degré ≥ 1, alors forcément son contenu est égal à 1 et donc P est irréductible dans $\mathbb{Q}[X]$ (lemme de Gauss). Inversement si P est irréductible dans $\mathbb{Q}[X]$ alors il existe $n \in \mathbb{Q}$ tel que $nP \in \mathbb{Z}[X]$ et de contenu égal à 1 ; nP est irréductible alors dans $\mathbb{Z}[X]$.
3. Soit $P(X) = aX^3 + bX^2 + cX + d \in \mathbb{Z}[X]$. D'abord, pour qu'il soit irréductible il faut que $pgcd(a, b, c, d) = 1$; s'il est réductible dans $\mathbb{Q}[X]$ alors il a une racine (car degré 3) : si $\frac{m}{n} \in \mathbb{Q}$ est une racine de P (avec $(n, m) = 1$) alors n divise a et m divise d. On teste alors tous les diviseurs de a et de d pour trouver la racine éventuelle.
4. Le polynôme $PY + Q$ est de contenu égal à 1 dans $K[X][Y]$; il est irréductible dans $K[X][Y]$ si et seulement si il est irréductible dans $K(X)[Y]$. Or le degré de $PY + Q$ en tant que polynôme en Y est égal à 1, il est donc irréductible.
5. Si $P = X^4 - \alpha^2$ alors P est évidement réductible. C'est en particulier le cas si P a une racine dans $\mathbb{Q}$. Supposons P réductible : il existe alors $b, c, b', c' \in \mathbb{Z}$ tels que $P = (X^2+bX+c)(X^2+b'X+c')$ ce qui implique que $b = b'$, $c + c' = b^2$, $b(c - c') = 0$ et $cc' = -a$. Si $b = 0$ alors $c = -c'$ et donc a est un carré ce qui revient au premier cas. Si $c = c'$, $a = -c^2$ (a est négatif), et $2c = b^2$; donc b^2 doit être pair et b est de la forme $b = 2d$. Donc $c^2 = 4d^4$ et $a = -4d^4$. On conclut que P est irréductible si et seulement si a est un carré ou a est de la forme $a = -4d^4$.
Pour $X^4 - aX - 1$, on remarque d'abord que si α est une racine alors α divise 1 donc les seules possibles racines dans $\mathbb{Z}$ sont -1 et 1 ; on a alors que P a une racine si et seulement si $a = 0$. Si $a \neq 0$, $P = (X^2 + bX + c)(X^2 + b'X + c') = X^4 - aX - 1$ implique $b = b'$, $c' + c = b^2$, $b(c' - c) = -a$ et $cc' = -1$; mais $c, c' \in \mathbb{Z}$ donc on $c + c' = 0$ et $b^2 = 0$ ce qui implique que $a = 0$ et P a une racine, donc est réductible. On a alors P irréductible si et seulement si $a \neq 0$.

EXERCICE 13. Montrer que les polynômes suivants sont irréductibles.

1. pour $n > 0$ et p premier, $X^n - p$ dans $\mathbb{Q}$.
2. $X^4 + X + 1$ dans $\mathbb{Q}$.
3. $X^6 + X^2 + 1$ dans $\mathbb{Q}$.
4. pour $n > 0$, $X^n - T$ dans $K(T)$ (K un corps).
5. $1 + X + \ldots + X^{p-1}$ sur $\mathbb{Q}$, pour p premier.

SOLUTION.

1. pour $n > 0$ et p premier, $X^n - p$ est irréductible dans $\mathbb{Q}[X]$ (grâce au critère d'Einsentein).
2. $P(X) = X^4 + X + 1$ est un polynôme primitif à coefficients dans $\mathbb{Z}$; il est donc irréductible dans $\mathbb{Q}[X]$ si et seulement s'il est irréductible dans $\mathbb{Z}[X]$. On regarde P modulo 2 : $P(0) = 1 \neq 0$ et $P(1) \neq 0$ donc on sait que, modulo 2, P n'a pas de facteurs de degré 1. Supposons $P(X) = (X^2 + aX + c)(X^2 + bX + 1) = X^4 + (a + b)X^3 + (2 + ab)X^2 + (a + b)X + (a + b)X + 1$ alors $a + b = 0$, $ab = -2$, $a + b = -1$ mais il n'y a pas de solution dans $\mathbb{Z}/2\mathbb{Z}$. Le polynôme P est alors irréductible dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$.
3. On regarde $P(X) = X^6 + X^2 + 1$ dans $\mathbb{Z}/2\mathbb{Z}[X]$: on a $P(X) = (X^3 + X + 1)^2$ et $X^3 + X + 1$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$. Si on regarde P dans $\mathbb{Z}/3\mathbb{Z}[X]$: $P = (X^2 - 1)(X^4 + X - 1)$ car $P(-1) = P(1) = 0$ donc on peut factoriser par $X + 1$ et $X - 1$. De plus $X^4 + X - 1$ est irréductible dans $\mathbb{Z}/3\mathbb{Z}$ car il n'a pas de racines et il n'est pas divisible par $X^2 + 1$, $X^2 + X - 1$ ou $X^2 - X - 1$ qui sont les polynômes de degré 2 de $\mathbb{Z}/3\mathbb{Z}$. On conclut donc que P n'admet pas de diviseurs de degré 1 ou 2 dans $\mathbb{Z}[X]$ (sinon il aurait par projection dans $\mathbb{Z}/2\mathbb{Z}[X]$) ni de diviseur de degré 3 (sinon il en aurait un par projection dans $\mathbb{Z}/3\mathbb{Z}[X]$). P est donc irréductible dans $\mathbb{Z}[X]$.
4. pour $n > 0$, $X^n - T$ dans $K(T)$ (K un corps) : il est irréductible dans $K(T)[X]$ grâce au critère d'Einsentein car T un élément irréductible de $K[T]$.
5. $P(X) = 1 + X + \ldots + X^{p-1}$ sur $\mathbb{Q}$, pour p premier. Si on pose $Y = X + 1$ on a $P = \frac{X^p - 1}{X - 1} = \sum_{i=0}^{p-1} C_p^{i+1} Y^i$ qui est irréductible par Einsentein : p divise C_p^{i+1} pour tout $i = 0, \ldots, p - 1$, p^2 ne divise pas C_p^1.

EXERCICE 14. On considère le nombre complexe

$$\zeta := e^{2\pi i/3}$$

et l'on définit un sous-groupe additif de $\mathbb{C}$ en posant :

$$R := \mathbb{Z} + \mathbb{Z}\zeta.$$

1. Montrer que R est un sous-anneau de $\mathbb{C}$, puis que R est isomorphe, en tant qu'anneau, à $\mathbb{Z}[X]/(X^2 + X + 1).\mathbb{Z}[X]$.
2. Etablir la majoration :
$$\sup_{z \in \mathbb{C}} \inf_{\alpha \in R} |z - \alpha| < 1.$$
[Il est recommandé de tracer une figure.]
3. Montrer que R est un anneau euclidien.
Quel est le groupe mutiplicatif $R^\times$ des unités de R ?
4. Dans la suite de cette partie, on désigne par p un nombre premier et l'on note $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.
Montrer qu'il existe des isomorphismes d'anneaux
$$R/p.R \cong \mathbb{Z}[X]/(p, X^2 + X + 1) \cong \mathbb{F}_p[X]/(X^2 + X + 1)\mathbb{F}_p[X],$$
où l'on a posé :
$$(p, X^2 + X + 1) := p.\mathbb{Z}[X] + (X^2 + X + 1)\mathbb{Z}[X].$$
5. Montrer que, si $p \neq 3$, les conditions suivantes sont équivalentes :
   (a) Le polynôme $X^2 + X + 1$ admet un racine dans $\mathbb{F}_p$.

(b) Le polynôme $X^3 - 1$ admet une racine $\neq 1$ dans $\mathbb{F}_p^\times$.

(c) $p \equiv 1 \pmod 3$.

6. Montrer que, si $p \neq 3$, les conditions suivantes sont équivalentes :

(a) $p \equiv 1 \pmod 3$.

(b) p n'est pas premier dans R.

(c) Il existe (x, y) dans $\mathbb{Z}^2$ tel que $p = x^2 - xy + y^2$.

7. Dans R, 3 est-il un élément premier ?

SOLUTION.

1. C'est assez clair que R est un sous-anneau de $\mathbb{C}$. On remarque que ζ est racine du polynôme $P(X) = X^2 + X + 1$. Si $\phi : \mathbb{Z}[X] \to \mathbb{C}$ est le morphisme d'anneau défini par : $\phi(X) = \zeta$, il se factorise par l'idéal engendré par P dans $\mathbb{Z}[X]$ et $\mathbb{Z}[X]/(P)$ est isomorphe à l'image de ϕ. L'image de ϕ est le sous-anneau de $\mathbb{C}$ engendré par ζ ; comme ζ vérifie $\zeta^2 = -\zeta - 1$, tout élément de R est combinaison linéaire dans $\mathbb{Z}$ de 1 et ζ, on montre facilement que l'image est égale à R. Et R est isomorphe, en tant qu'anneau, à $\mathbb{Z}[X]/(X^2 + X + 1).\mathbb{Z}[X]$.

2. En dessinant R dans $\mathbb{C}$, on montre que tout nombre complexe z est à une distance strictement inférieure à $\frac{\sqrt{3}}{3}$ donc < 1. Et donc $\sup_{z\in\mathbb{C}} \inf_{\alpha\in R} |z - \alpha| < 1$.

3. On montre alors facilement que R est un anneau euclidien pour le stathme défini par

$$N(a + \zeta b) = (a + \zeta b)(\overline{a + \zeta b}) = a^2 - ab + b^2$$

où pour $z \in \mathbb{C}$ on note $\overline{z}$ le conjugué complexe de z. Si $x = a + \zeta b$ et $y = c + \zeta d$ sont deux éléments non nuls de R, considérons $z = \frac{a+\zeta b}{c+\zeta d}$ qui est un élément de $\mathbb{C}$. Si $z = \alpha \in R$, alors $x = y\alpha + r$, avec $r = 0$. Sinon, soit $\alpha \in R$ tel que $|z - \alpha| < 1$ (qui existe d'après la question précédente). On pose alors $r = x - y\alpha$ qui est un élément de R vérifiant $|\frac{r}{y}| = |\frac{x}{y} - \alpha| < 1$; ceci implique que $|r| < |y|$ et donc $N(r) < N(y)$. On a donc bien $x = y\alpha + r$, $\alpha \in R$, $N(r) < N(y)$ ou $r = 0$.
Le groupe multiplicatif $R^\times$ des unités de R est égale à $\{\pm(1+\zeta), \pm\zeta, \pm 1\}$. On le trouve en montrant que les inversibles de R sont exatement les $\alpha \in R$ tels que $N(\alpha) = 1$.

4. Dans la suite de cette partie, on désigne par p un nombre premier et l'on note $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.
Grâce au cours on sait qu'il existe des isomorphismes d'anneaux

$$R/p.R \cong \mathbb{Z}[X]/(p, X^2 + X + 1) \cong \mathbb{F}_p[X]/(X^2 + X + 1)\mathbb{F}_p[X],$$

oùl'on a posé :

$$(p, X^2 + X + 1) := p.\mathbb{Z}[X] + (X^2 + X + 1)\mathbb{Z}[X].$$

5. On va supposer que $p > 3$.
a) implique b) : Comme $X^3 - 1 = (X - 1)(X^2 + X + 1)$, si $z^2 + z + 1 \equiv 0[p]$, alors $z^3 - 1 \equiv 0[p]$ (et $z \neq 1$ car 1 n'est pas une racine de $X^2 + X + 1$ modulo p).
b) implique c) : s'il existe $z \in \mathbb{F}_p$ tel que $z^3 \equiv 1[p]$ alors 3 doit forcément diviser l'ordre du groupe $\mathbb{F}_p^*$ qui est $p - 1$ donc $p - 1 \equiv 0[p]$.
c) implique a) : Si $p \equiv 1[3]$, alors 3 divise $p - 1$ et par le lemme de Cauchy il existe un élément $z \in \mathbb{F}_p^*$ différent de l'élément neutre tel que $z^3 \equiv 1[p]$. z est donc une racine de $X^2 + X + 1$ modulo p.

6. Si $p > 3$, montrons a) implique b) : Si $p \equiv 1[3]$ alors le polynôme $X^2 + X + 1$ admet une racine modulo p, $z \not\equiv 1[p]$ d'après la question 5. Donc $P(X) = X^2 + X + 1$ est réductible dans $\mathbb{F}_p[X]$. L'idéal engendré par (P) n'est alors pas premier, ce qui implique que p n'est pas premier dans R (qui est factoriel car euclidien).
   b) implique c) : p non premier alors il existe $a = x + \zeta y, b = x' + \zeta y' \in R$ non inversibles tels que $p = ab$. Donc

$$N(p) = N(ab) = N(a)N(b) = [(x-\frac{y}{2})^2+\frac{3}{4}y^2][(x'-\frac{y'}{2})^2+\frac{3}{4}y'^2] = (x^2-xy+y^2)(x'^2-x'y'+y'^2);$$

   comme $N(p) = p^2$, on a $p^2 = (x^2 - xy + y^2)(x'^2 - x'y' + y'^2)$. Donc $x^2 - xy + y^2$ divise p^2 : c'est donc égal soit à p^2 mais dans ce cas $x'^2 - x'y' + y'^2 = N(b) = 1$ ce qui est faux, car b est non inversible, soit à p et dans ce cas on a bien $x, y \in \mathbb{Z}$ tels que $p = x^2 - xy + y^2$.
   c) implique a) : On suppose que $p \equiv 2[3]$ et on regarder $x^2 - xy + y^2$ modulo 3 : les seules valeurs possibles pour $x^2 - xy + y^2$ modulo 3 sont 0, 1 (on essaye tous les couples (x, y) possibles modulo 3), donc pour $x, y \in \mathbb{Z}$, $p \not\equiv x^2 - xy + y^2[3]$ donc a fortiori, $p \neq x^2 - xy + y^2$.
7. Dans R, 3 n'est pas un élément premier car $X^2 + X + 1$ n'est pas irréductible dans $\mathbb{F}_3[X]$.