Correction 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 $P(X,Y) \in \mathbf{Z}[X,Y]$ est tel que $P\left(t^2,t^3\right) = 0$ pour tout $t \in \mathbf{Z}$ si, et seulement si, il existe un polynôme $Q(X,Y) \in \mathbf{Z}[X,Y]$ tel que $P(X,Y) = (X^3 - Y^2)\cdot Q(X,Y)$. En déduire un isomorphisme de $\mathbf{Z}$-algèbres

$$\mathbf{Z}[X,Y]/\left(X^3-Y^2\right) \cong \{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\} \cong \mathbf{Z}[T^2,T^3].$$

Solution. Commençons par préciser que l'on peut toujours effectuer une division euclidienne dans $k[X]$ pour k corps avec unicité du quotient et du reste. On a vu dans l'exercice 10 du TD III que l'on peut toujours effectuer une division euclidienne (en perdant l'unicité cependant) de P par Q dans $A[X]$ à condition que le coefficient dominant de Q soit inversible[1] dans A. Si jamais le coefficient dominant de Q n'est pas inversible, alors on peut parfois s'en sortir en voyant $A[X] \subseteq \mathrm{Frac}(A)[X]$ et effectuer le division euclidienne dans $\mathrm{Frac}(A)[X]$. Par exemple, soient $P, Q \in A[X,Y] = A[X][Y]$. Si le coefficient dominant de Q vu dans $A[X][Y]$ n'est pas dans $A[X]^\times = A^\times$, alors on effectue la division dans $A(X)[Y]$, ce qui fournit $B, R \in A[X,Y]$ avec $\deg_Y(R) < \deg_Y(Q)$ et $A \in A[X]$ non nul tel que $A(X)P(X,Y) = Q(X,Y)B(X,Y) + R(X,Y)$.

Venons-en alors à l'exercice à proprement parler. Il est immédiat que si $P \in (X^3-Y^2)$, alors pour tout entier relatif t, $P(t^2,t^3) = 0$. Réciproquement, supposons que pour tout entier relatif t, $P(t^2,t^3) = 0$. le coefficient dominant de[2] $X^3 - Y^2 \in \mathbf{Z}[X][Y]$ est égal à $-1 \in \mathbf{Z}^\times = \mathbf{Z}[X]^\times$. On peut donc effectuer une division euclidienne de P par $X^3 - Y^2$ si bien qu'il existe $Q, R \in \mathbf{Z}[X,Y]$ avec $\deg_Y(R) < 2$ tels que $P(X,Y) = (X^3-Y^2)Q(X,Y) + R(X,Y)$. Puisque $\deg_Y(R) < 2$, il existe $A, B \in \mathbf{Z}[X]$ tels que $R(X,Y) = A(X)Y + B(X)$ de sorte que $P(X,Y) = (X^3-Y^2)Q(X,Y) + A(X)Y + B(X)$. On peut alors évaluer cela en $t \in \mathbf{Z}$ pour obtenir que

$$0 = P(t^2,t^3) = (t^6-t^6)Q(t^2,t^3) + A(t^2)t^3 + B(t^2) = A(t^2)t^3 + B(t^2).$$

On en déduit (puisque $\mathbf{Z}$ est infini) que $A(X^2)X^3 + B(X^2) = 0$. On voit que $A(X^2)X^3$ ne fait intervenir que des monômes impairs distincts et que $B(X^2)$ ne fait intervenir que des monômes pairs distincts. On en déduit que $A = B = 0$ et donc $R = 0$ et $P \in (X^3-Y^2)$ et on a bin démontré l'équivalence.
On pose alors $\mathbf{Z}[T^2,T^3] = \{P(T^2,T^3) \ : \ P \in \mathbf{Z}[X,Y]\}$ et on considère le morphisme surjectif de $\mathbf{Z}$-algèbre $f : \mathbf{Z}[X,Y] \to \mathbf{Z}[T^2,T^3]$ définie par $P \mapsto P(T^2,T^3)$. Ce qui précède garantit que le noyau est égal à l'idéal (X^3-Y^2) si bien qu'au quotient on a bien

$$\mathbf{Z}[X,Y]/\left(X^3-Y^2\right) \cong \mathbf{Z}[T^2,T^3].$$

Reste donc à voir que $\{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\} \cong \mathbf{Z}[T^2,T^3]$. On a évidemment $\mathbf{Z}[T^2,T^3] \subseteq \{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\}$ puisqu'un tel polynôme n'a pas de terme en T. Réciproquement, si $P \in \{P \in \mathbf{Z}[T] \ : \ P'(0) = 0\}$, alors il existe un $d \in \mathbf{N}$ tel que

$$P = \sum_{\substack{i=0 \\ i\neq 1}}^{d} a_i T^i.$$

Mais pour tout $i \neq 1$, on peut effectuer la division euclidienne de i par 3 pour obtenir l'existence de $q \in \mathbf{Z}$ et $r \in \{0,1,2\}$ tel que $i = 3q + r$. Si $r = 0$, alors $T^i = (T^3)^q$ tandis que si $r = 2$, alors $T^i = (T^3)^q T^2$. Enfin, si $r = 1$, on a $i = 3(q-1)+4$ et $T^i = (T^3)^{q-1}(T^2)^2$ qui a bien un sens car $q - 1 \geqslant 0$ puisque sinon $q = 0$ et $r = 1$ donc $i = 1$ ce qui est exclu. On a donc bien que $P \in \mathbf{Z}[T^2,T^3]$, ce qui conclut la démonstration. On pouvait aussi traiter les cas i pairs d'un côté et les $i \geqslant 3$ impairs en remarquant que $i - 3$ est positif et pair.

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

$$I_1 := (P) = P\cdot A \quad \text{et} \quad I_2 := \{Q \in k[X_1,\dots,X_N] \mid Q(\mathbf{a}) = 0\}.$$

Montrer que I_1 et I_2 sont des idéaux étrangers si, et seulement si, $P(\mathbf{a}) \neq 0$. On rappelle que, par définition, I_1 et I_2 sont des idéaux étrangers de A si $I_1 + I_2 = A$.

1. Voir le lemme 3.31 du Perrin pour une démonstration.
2. Noter que ce choix est plus judicieux que $A[Y][X]$ car le degré en Y de $X^3 - Y^2$ est strictement inférieur à son degré en X.

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 $\mathbf{Z}_{(p)}$ la localisation de $\mathbf{Z}$ par rapport à l'idéal premier (p). Montrer que $\mathbf{Z}_{(p)}$ 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 $\mathbf{R}$ contenant 0 et $f : U \longrightarrow \mathbf{R}$ 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 $A = \mathbf{Z}$ 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 $\mathbf{Z}$ n'est pas local car pour tout nombre premier p, l'idéal $p\mathbf{Z}$ 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, $\mathbf{Z}_{(p)} = S^{-1}\mathbf{Z}$ où $S = A\backslash(p)$ qui est une partie multiplicative de $\mathbf{Z}$. On a déjà montré que l'idéal engendré par l'image de (p) était le seul idéal maximal de $\mathbf{Z}_{(p)}$ (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 $Q \in \mathbf{Z}[X]$ unitaire. On note $z_1, ..., z_n$ ses racines (pas forcément distinctes) dans $\mathbf{C}$. Montrer que

$$\prod_{i \neq j} (z_i - z_j) \in \mathbf{Z}.$$

Solution. On observe que le polynôme en n indéterminées

$$P = \prod_{i \neq j} (X_i - X_j)$$

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

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

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

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

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

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

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 :

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

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 $d \in \mathbf{Z}$ un entier sans facteur carré non nul. On pose :

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

Montrer que si $d \equiv 1 \pmod 4$, alors $\mathbf{Z}[\sqrt{d}]$ n'est pas intégralement clos.
Indication : Considérer l'élément $\frac{1+\sqrt{d}}{2}$.

Solution.

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

2. 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

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

donc $p^n = -a_{n-1} p^{n-1} q - \cdots - a_1 p q^{n-1} - a_0 q^n$, 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 $x = pq^{-1} \in A$.

3. 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 $\mathbf{Z}[\sqrt{d}]$ 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 $n \in \mathbf{N}$.

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

Solution.

1. Pour tout monôme non constant
$$S = \lambda X_0^{\alpha_0} X_1^{\alpha_1} \cdots X_r^{\alpha_r} \in K[X_0, \ldots, X_r]$$
(avec $\lambda \in K$), on a $R := S(X, XY, \ldots, XY^r)$ 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 $I := (X, XY, \ldots, XY^r)$ est inclus dans l'idéal $J := (X, XY, \ldots, XY^r, XY^{r+1})$. Montrons que l'inclusion est stricte en vérifiant que $XY^{r+1} \notin I$. Sinon, on pourrait écrire
$$XY^{r+1} = P_0 X + \cdots + P_r XY^r,$$
où les P_i sont dans B. Comme l'anneau $B \subset K[X, Y]$ est intègre, on aurait
$$Y^{r+1} = P_0 + \cdots + P_r Y^r.$$
En faisant $X = 0$ et en appliquant a), on aurait des élèments $\lambda_0, \ldots, \lambda_r$ de K tels que
$$Y^{r+1} = \lambda_0 + \cdots + \lambda_r Y^r,$$
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 $R_1 = P_1/Q_1, \ldots, R_s = P_s/Q_s$ des éléments de F, avec $P_i \in k[X]$ et Q_i non nul dans $k[X]$ pour tout i de $\{1, \ldots, s\}$. Soit B la sous-k-algèbre de F engendrée par $R_1, \ldots, R_s$. Montrer qu'il existe un polynôme non nul $G \in k[X]$ tel que $B \subseteq (k[X])[G^{-1}]$.
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 $Q_1^{\alpha_1} \cdots Q_r^{\alpha_r}$, où les α_i sont dans $\mathbf{N}$. Il suffit alors de prendre $G = Q_1 \cdots Q_r$.
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 — Artin-Tate. 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-espace vectoriel 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 $\alpha_1, \ldots, \alpha_n$ dans B tels que $B = A[\alpha_1, \ldots, \alpha_n]$.

1. Soit $\beta_1, \ldots, \beta_m$ 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. Soit B' l'ensemble des éléments 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

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

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

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

en les β_j est dans B'. Or, d'après 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 $\beta_1^{s_1} \cdots \beta_m^{s_m}$ 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 $(\beta_1, \ldots, \beta_m)$ du L-ev B, on obtient $y \in C$. Finalement $L = C$, et L est bien de type fini comme A-algèbre.

Exercice 9 — Lemme de Zariski. 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-espace vectoriel de dimension finie. Pour cela on écrit $K = k[\alpha_1, \ldots, \alpha_n]$, et on raisonne par récurrence en supposant le résultat vrai jusqu'à $n-1$, le cas $n = 0$ étant trivial.

1. On pose[3] $L = k(\alpha_1)$. Comparer K et $L[\alpha_2, \ldots, \alpha_n]$, 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.

Solution.

1. Comme K est un corps, il contient $k(\alpha_1)$, et donc aussi $L[\alpha_2, \ldots, \alpha_n]$. Comme par hypothèse $K = k[\alpha_1, \ldots, \alpha_n]$, on a finalement $K = L[\alpha_2, \ldots, \alpha_n]$, 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 3 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 $k[\alpha_1] = k(\alpha_1) = \mathrm{Vect}_k(1, \alpha_1, \ldots, \alpha_1^{d-1})$ 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 — Théorème des zéros de Hilbert. Cet exercice utilise le résultat de l'exercice 9. Soit k un corps.

1. Soient $a_1, \ldots, a_n$ dans k. Montrer que le morphisme $u : P \mapsto P(a_1, \ldots, a_n)$ de $k[X_1, \ldots, X_n]$ dans k est surjectif de noyau l'idéal $J = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$.

On suppose dans la suite que k est algébriquement clos et on se donne I un idéal maximal de $k[X_1, \ldots, X_n]$.

2. Montrer que le corps $L = k[X_1, \ldots, X_n]/I$ est isomorphe (en tant que k-algèbre) à k.
Indication : On appliquera le résultat principal de l'exercice 8.

3. En déduire qu'il existe $a_1, \ldots, a_n$ dans k tel que I soit l'idéal J du **1.**, c'est-à-dire que I est l'ensemble des polynômes $P \in k[X_1, \ldots, X_n]$ tels que $P(a_1, \ldots, a_n) = 0$.

3. C'est le corps des fractions de $k[\alpha_1]$.

Solution.

1. Le morphisme u est surjectif (prendre P constant). Si maintenant $P \in k[X_1, \dots, X_n]$, on peut faire la division euclidienne de P par $(X_1 - a_1)$ dans l'anneau $(k[X_1])[X_2, \dots, X_n]$, ce qui permet d'écrire $P = Q_1(X_1 - a_1) + R$ avec $R \in k[X_2, \dots, X_n]$. Par récurrence, on peut écrire $P = Q_1(X_1 - a_1) + \cdots + Q_n(X_n - a_n) + b$ 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 $(x^n)_{n\in\mathbf{N}}$ 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 $k \longrightarrow k[X_1, \dots, X_n]/I$ est un isomorphisme. Soient $a_1, \dots, a_n$ les antécédents de $X_1, \dots, X_n$, 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), $k[X_1, \dots, X_n]/J$ 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 $[0,1] \longrightarrow \mathbf{R}$ n'est pas noethérien. Pour ce faire, on montrera que l'idéal des fonctions s'annulant en 0 n'est pas finiment engendré.

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 que $\{x_0\}$ n'est pas ouvert et pour $n \geqslant 1$, soit $f_n : x \in X \longrightarrow d(x, x_0)^{\frac{1}{n!}}$ où d désigne la distance dans[4] X. Si on pose I_n l'idéal engendré par f_n dans A, alors la suite $(I_n)_{n\in\mathbf{N}}$ est une suite croissante[5] d'idéaux de A qui ne stationne pas[6]. Donc $\{x_0\}$ est forcément ouvert et X est discret. A est donc isomorphe à $\mathbf{R}^X$, les applications de X dans $\mathbf{R}$ qui est noethérien si X est fini.
Réciproquement, si X est fini alors $A = C^0(X)$ est isomorphe à $\mathbf{R}^X$ qui est noethérien.

Exercice 12.

1. Soit A un anneau factoriel, et soit K le corps des fractions de A. Donner un exemple de polynôme réductible dans $A[X]$ et irréductible dans $K[X]$ et un exemple de polynôme irréductible dans $A[X]$ et réductible dans $K[X]$.
2. Donner les éléments irréductibles de $\mathbf{Z}[X]$ en fonction de ceux de $\mathbf{Q}[X]$ et de $\mathbf{Z}$.
3. Donner une procédure permettant de déterminer si un polynôme de degré au plus 3 est irréductible dans $\mathbf{Z}[X]$.
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 $a \in \mathbf{Z}$. À quelle condition $X^4 - a$ est-il irréductible dans $\mathbf{Q}[X]$? et $X^4 - aX - 1$ dans $\mathbf{Z}[X]$?

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 constant irréductible de $A[X]$ qui n'est pas primitif.

4. On a en effet, pour tous $x, y \in X$, que
$$|d(x, x_0) - d(y, x_0)| \leqslant d(x, y)$$
ce qui établit que f_n est continue sur X. On peut aussi raisonner en remarquant que l'image réciproque d'un ouvert est ouverte.

5. Car pour tout $n \in \mathbf{N}$, $f_n = (f_{n+1})^{n+1}$.

6. C'est ici que l'hypothèse $\{x_0\}$ non ouvert intervient. En effet, sinon $f_{n+1} \in I_n$ et il existerait une fonction continue f telle que $f_{n+1} = f f_n$ soit $f_n = f^{n+1} f_n^{n+1}$. On en déduit pour tout $x \neq x_0$ que $f^{n+1} = \frac{1}{f_n^n}$. Mais le fait que $\{x_0\}$ ne soit pas ouvert implique qu'il existe une suite $(y_k) \in X^{\mathbf{N}}$ telle que $\lim\limits_{k\to+\infty} d(x_0, y_k) = 0$. On a donc une contradiction puisque f^{n+1} est continue en x_0 et $\lim\limits_{k\to+\infty} |f|^{n+1} = +\infty$. Noter que dans le cas où $\{x_0\}$ est ouvert, la fonction f définie pour tout $x \neq x_0$ par $x \mapsto \frac{1}{d(x_0,x)}$ et $f(x_)) = 0$ est continue sur X. C'est clair sur $X \setminus \{x_0\}$ et comme il existe $r_0 > 0$ tel que $d(x_0, x) < r_0 \Rightarrow x = x_0$ par caractère ouvert,
$$\forall \varepsilon > 0, \quad \exists r_0 > 0 \quad \text{tel que} d(x_0, x) < r_0 \Rightarrow |f(x) - f(x_0)| = 0 < \varepsilon.$$

2. Un nombre premier $p \in \mathbf{Z}$ est irréductible dans $\mathbf{Z}[X]$ comme polynôme de degré 0. Si P est un polynôme irréductible de $\mathbf{Z}[X]$ de degré $\geqslant 1$, alors forcément son contenu est égal à 1 et donc P est irréductible dans $\mathbf{Q}[X]$ (lemme de Gauß). Inversement si P est irréductible dans $\mathbf{Q}[X]$ alors il existe $n \in \mathbf{Q}$ tel que $nP \in \mathbf{Z}[X]$ et de contenu égal à 1 ; nP est alors irréductible dans $\mathbf{Z}[X]$.

3. Soit $P(X) = aX^3 + bX^2 + cX + d \in \mathbf{Z}[X]$. D'abord, pour qu'il soit irréductible il faut que $\text{pgcd}(a, b, c, d) = 1$; s'il est réductible dans $\mathbf{Q}[X]$ alors il a une racine (car degré 3) : si $\frac{m}{n} \in \mathbf{Q}$ 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[7].

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 évidemment réductible. C'est en particulier le cas si P a une racine dans[8] $\mathbf{Q}$. Supposons P réductible : il existe alors $b, c, b', c' \in \mathbf{Z}$ 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 réductible 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 racines possibles dans $\mathbf{Z}$ 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 $c, c' \in \mathbf{Z}$ 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, $X^n - p$ sur $\mathbf{Q}$;

2. $X^4 + X + 1$ sur $\mathbf{Q}$;

3. $X^6 + X^2 + 1$ sur $\mathbf{Q}$;

4. Pour $n > 0$, $X^n - T$ sur $K(T)$ (K un corps) ;

5. $1 + X + \ldots + X^{p-1}$ sur $\mathbf{Q}$, pour p premier.

Solution.

1. On applique le critère d'Eisenstein avec p.

2. On peut raisonner comme dans l'exercice précédent questions **3.** et **5**. On commence par montrer que l'on n'a pas de racine dans $\mathbf{Q}$ car une telle racine $\frac{p}{q}$ vérifierait $q = \pm 1$ et $p = \pm 1$ mais ni 1 ni -1 n'est racine. On raisonne alors par l'absurde et on voit qu'on n'a aucune factorisation du type $(X^2 + aX + b)(X^2 + cX + d)$.
Une autre preuve est fournie dans le Perrin page 78.

3. Plusieurs méthodes sont possibles. Attention que le fait que $X^3 + X + 1$ soit irréductible sur $\mathbf{Q}$ (car sans racine et de degré $\leqslant 3$) implique que $X^6 + X^2 + 1$ est sans racine rationnelle mais pas qu'il est irréductible[9]. On peut alors raisonner par l'absurde et montrer qu'on n'a aucune factorisation du type $(X^2 + aX + b)(X^4 + cX^3 + dX^2 + eX + f)$ (ce qui implique en particulier l'abscence de factorisation comme un produit de trois polynômes de degré 2) ni de la forme $(X^3 + aX^2 + bX + d)(X^3 + eX^2 + fX + g)$ mais c'est un peu fastidieux.
On pouvait sinon raisonner modulo certains nombres premiers. On voit tout de suite que $X^6 + X^2 + 1 = (X^3 + X + 1)^2$ dans $\mathbf{F}_2$ et on vérifie que $X^3 + X + 1$ y est irréductible (car de degré 3 sans racine). Ceci nous fournit[10] que $X^6 + X^2 + 1$ est soit irréductible sur $\mathbf{Q}$ soit est un produit de deux polynômes de degré 3. Mais, on vérifie que dans $\mathbf{F}_3$ on a deux racines

7. Je rappelle qu'un polynôme de degré 2 ou 3 est irréductible sur un corps k si, et seulement s'il n'a pas de racine. La condition nécessaire est évidente et pour la condition suffisante, il suffit de voir qu'un polynôme de degré 2 ou 3 non irréductible s'écrit comme produit de polynômes irréductibles de degré strictement inférieur et que cela fait nécessairement apparaître si $\deg(P) \leqslant 3$ un polynôme irréductible de degré 1 donc une racine !

8. On pouvait ici utiliser la factorisation sur $\mathbf{C}[X]$ et déterminer pour quelles valeurs de a, cela fournissait soit une racine rationnelle soit un produit de deux polynômes de degré 2 à coefficients rationnels.

9. Par exemple, $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$ est réductible mais $X^2 + 4$ est irréductible.

10. En effet, $P = X^6 + X^2 + 1$ est primitif et si on écrit sa factorisation en produit d'irréductibles dans l'anneau factoriel $\mathbf{Z}[X]$, alors on obtient des polynômes irréductibles de $\mathbf{Z}[X]$ de degré $\geqslant 1$ donc primitifs et irréductibles sur $\mathbf{Q}[X]$. Par unicité (aux unités près) d'une telle décomposition, on peut donc supposer que la décomposition de P en produit d'irréductibles est de la forme

$$P = \prod_{i=1}^{r} P_i^{n_i}$$

avec les P_i des polynômes irréductibles de $\mathbf{Z}[X]$ unitaires non constants et 2 à deux non associés. Soit alors p un nombre premier et $\overline{P}$ le polynôme obtenu

(à savoir ± 1) si bien que $X^6 + X^2 + 1 = (X-1)(X+1)Q$ avec Q de degré 4 sans racine [11] dans $\mathbf{F}_3$. Cela implique que $X^6 + X^2 + 1$ est irréductible. En effet, on a vu modulo 2 que soit P est irréductible soit il est produit de deux irréductibles de degré 3. Mais la réduction modulo 3 de P s'écrirait alors comme un produit de deux polynômes de degré 3. La seule possibilité pour obtenir une décomposition de la forme $(X-1)(X+1)Q$ avec Q de degré 4 sans racine est que chaque polynôme de degré 3 se scinde en un polynôme de degré 1 fois un polynôme irréductible de degré 2 et cela impliquerait en particulier que $Q = X^4 + X^2 + 2$ est produit de deux polynômes irréductibles uniatires de degré 2 sur $\mathbf{F}_3[X]$. Mais un polynôme unitaire de degré 2 irréductible sur $\mathbf{F}_3[X]$ est de la forme $X^2 + aX + b$ sans racine. Notamment cela impose $b \neq 0$. Testant alors toutes les combinaisons possibles de $a, b \in \mathbf{F}_3$, on constate que les seuls polynômes irréductibles unitaires de degré 2 sur $\mathbf{F}_3[X]$ sont X^2+1, X^2+X-1 et X^2-X-1. On vérifie alors qu'aucun produit de deux de ces polynômes de fournit Q. On en conclut que P n'est pas produit de deux irréductibles de degré 3 et que par conséquent P est irréductible [12].

Remarque : On a notamment que s'il existe p premier tel que $\overline{P}$ soit irréductible modulo p, alors P est irréductible sur $\mathbf{Q}$. Attention en revanche qu'un tel p n'existe pas toujours (on verra notamment que X^4+1 est irréductible sur $\mathbf{Z}$ mais réductible modulo tout premier p. cela a à voir encore une fois avec le groupe de Galois de P. Vous pourrez trouver des compléments dans le chapitre 4 du cours ou en section III.3 du Perrin.
Terminons par mentionner que factoriser un polynôme sur un corps fini se fait très bien algorithmiquement via l'algorithme de Berlekamp et que cet algorithme et des réductions modulo des nombres premiers bien choisis (grâce aux bornes de Mignotte) permet d'obtenir un algorithme de factorisation sur $\mathbf{Z}$. Rendez-vous lors du cours de calcul formel du semestre prochain si ces thématiques vous intéressent !

4. L'élément T est irréductible dans l'anneau factoriel $K[T]$ et on peut lui appliquer le critère d'Eisenstein (comme en **1.**) qui fournit l'irréductibilité dans $K[T][X]$ et comme le polynôme est primitif, dans $K(T)[X]$.

5. On remarque qu'il s'agit du polynôme cyclotomique [13] Φ_p. On constate que $(X-1)\Phi_p = X^p - 1$ et en évaluant en $X+1$, il vient que $X\Phi_p(X+1) = (X+1)^p - 1$, autrement dit

$$\Phi_p(X+1) = X^{p-1} + \sum_{k=1}^{p-2} C_{k+1}^p X^k + p.$$

On remarque alors que [14] $p \mid C_{k+1}^p$ pour tout $k \in \{1, \dots, p-2\}$ et on peut alors déduire d'Eisenstein appliqué à p que le polynôme $\Phi_p(X+1)$ est irréductible, ce qui implique que Φ_p est irréductible lui-même [15].

Exercice 14. On considère le nombre complexe $\zeta := e^{2\pi i/3}$ et l'on définit un sous-groupe additif de $\mathbf{C}$ en posant $R := \mathbf{Z} + \mathbf{Z}\zeta$.

1. Montrer que R est un sous-anneau de $\mathbf{C}$, puis que R est isomorphe, en tant qu'anneau, à $\mathbf{Z}[X]/(X^2+X+1)$.

---

en réduisant modulo p les coefficients de P. On a (c'est un morphisme d'algèbres) que

$$\overline{P} = \prod_{i=1}^{r} \overline{P_i}^{n_i} = (X^3+X+1)^2.$$

Puisque les P_i sont unitaires, $\overline{P_i}$ a même degré que P_i. Si on avait un P_i irréductible de degré 2 dans la décomposition de P, alors on obtiendrait un facteur $\overline{P}_i$ de degré 2 qui est soit irréductible soit produit de deux polynômes irréductibles de degré 1, ce qui est exclu car on a un seul facteur irréductible de degré 3 de multiplicité 2. De même, si on avait un P_i de degré 1, alors on aurait une racine modulo p, ce qui n'est pas le cas. Les seuls types de factorisation possibles sont donc P irréductible ou P produit de deux polynômes irréductibles de degré 3.

11. Ici, on obtient le sans racine soit en utilisant que $Q = X^4 + X^2 + 2$ soit en utilisant le fait que sur un corps, x est racine multiple si, et seulement si, $P(x) = P'(x) = 0$ (même en caractéristique > 0). En effet, si $P = (X-x)^2 Q$, il est clair que $P(x) = P'(x) = 0$. Réciproquement (noter qu'en revanche la démonstration habituelle à base de formule de Taylor ne fonctionne plus), mais le fait que $P(x) = 0$ implique que $P = (X-x)Q$ et donc $P' = (X-x)Q' + Q$ et on voit que $P'(x) = 0$ équivaut à $Q(x) = 0$ et donc au fait que x soit racine multiple. Attention en revanche que du fait que la dérivée de X^p est nulle en caractéristique p que l'équivalence x est de multiplicité m si, et seulement si, $P(x) = P'(x) = \cdots = P^{(m-1)}(x) = 0$ et $P^{(m)}(x) \neq 0$ tombe en défaut ! En revanche, on peut établir que cela reste toutefois vrai si $m \leqslant p-1$.

12. On verra que les types de factorisation qui apparaissent modulo p et que l'on a utilisés ici sont liés aux groupes de Galois des polynômes !

13. On reviendra en détails sur ces polynômes importants dans le chapitre sur les corps. Ils sont par exemple à la base d'une démonstration d'une version faible du théorème de la progression arithmétique de Dirichlet stipulant qu'il existe une infinité de nombres premiers $p \equiv 1 \pmod{n}$ pour tout entier naturel n ou du théorème de Wedderburn stipulant que tout corps fini est commutatif.

14. Car pour $k \in \{1, \dots, p-2\}$, $p \mid (k+1)! C_{k+1}^p = p(p-1)\cdots(p-k)$ et $(k+1)!$ est premier à p.

15. Sinon, on a $\Phi_p = Q_1 Q_2$ avec Q_1 et Q_2 non constants si bien que $\Phi_p(X+1) = Q_1(X+1)Q_2(X+1)$ avec $Q_1(X+1)$ et $Q_2(X+1)$ non constants, ce qui est absurde.

2. Établir la majoration :

$$\sup_{z\in\mathbf{C}} \inf_{\alpha\in R} |z-\alpha| < 1.$$

Indication : 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 $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$.
Montrer qu'il existe des isomorphismes d'anneaux

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

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

(a) Le polynôme X^2+X+1 admet un racine dans $\mathbf{F}_p$;

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

(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 $\mathbf{Z}^2$ tel que $p = x^2 - xy + y^2$.

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

SOLUTION.

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

2. Voir le corrigé du DM I, question **6.** de l'exercice 3 dans la démonstration que l'anneau est euclidien. En dessinant R dans $\mathbf{C}$, on montre que tout nombre complexe z est à une distance strictement inférieure à $\frac{\sqrt{3}}{3}$ donc < 1. Et donc $\sup_{z\in\mathbf{C}} \inf_{\alpha\in R} |z-\alpha| < 1$.

3. Voir le corrigé du DM I, question **6.** de l'exercice 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 $z \in \mathbf{C}$ 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 $\mathbf{C}$. 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 exactement les $\alpha \in R$ tels que $N(\alpha) = 1$.

4. Voir le corrigé du DM I, question **5.** de l'exercice 3. Grâce au cours on sait qu'il existe des isomorphismes d'anneaux

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

où l'on a posé :

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

5. Puisque $X^3-1 = (X-1)(X^2+X+1)$, il est clair que $(a) \iff (b)$. Supposons alors (b). On a donc un élément $x \in \mathbf{F}_p^\times$ d'ordre 3 donc $3 \mid p-1$ par Lagrange et on a (c). Réciproquement, si $p \equiv 1 \pmod 3$, alors $3 \mid p-1 = \#\mathbf{F}_p^\times$ et par le lemme de Cauchy (ou les théorèmes de Sylow), on a un élément d'ordre 3, autrement dit une racine $\neq 1$ de X^3-1.

6. D'après **5.**, $p \equiv 1 \pmod 3$ équivaut au fait que $X^2 + X + 1$ soit scindé dans $\mathbf{F}_p$, ce qui équivaut au fait que

$$R/(p) \cong \mathbf{F}_p[X]/(X^2 + X + 1)$$

ne soit pas intègre et donc à ce que p ne soit pas premier dans R. On a donc $(a) \iff (b)$. Supposons alors (b), par factorialité et le fait que p ne soit pas irréductible, il existe z, z' des éléments de R qui ne sont pas des unités tels que $p = zz'$ si bien que $p^2 = N(Z)N(z')$ et le fait que z et z' ne soient pas des unités équivaut au fait que $N(Z), N(z') \notin \{\pm 1\}$ de sorte que $N(Z) = N(z') = p$. Écrivant $z = x + \xi y$ avec $x, y \in \mathbf{Z}$, il vient que $p = x^2 - xy + y^2$. Réciproquement, (c) fournit que $p = N(z)$ avec $z = x + \xi y$ et ainsi $p = z\overline{z}$ avec $N(z) = N(\overline{z}) = p \notin \{\pm 1\}$ de sorte que z et $\overline{z}$ ne sont pas des unités. Cela fournit que p n'est pas premier et donc (b), ce qui conclut la preuve.

7. On applique **4.** pour obtenir que $R/(3) \cong \mathbf{F}_3[X]/(X^2 + X + 1)$ et modulo 3, on a $X^2 + X + 1$ qui est réductible (car $X^2 + X + 1 = (X - 1)^2$) si bien que $R/(3)$ n'est pas intègre et (3) n'est pas premier !

Exercice 15 — Anneau des séries formelles. Soient k un corps et $\mathbf{R}^{\mathbf{N}}$ le groupe abélien des suites à valeurs dans k. On notera $\sum_{n=0}^{+\infty} a_n T^n$ formellement une telle suite $(a_n)_{n\in\mathbf{N}}$. On définit alors une loi de multiplication par produit de Cauchy

$$\left(\sum_{n=0}^{+\infty} a_n T^n\right) \times \left(\sum_{n=0}^{+\infty} b_n T^n\right) = \sum_{n=0}^{+\infty} \left(\sum_{i+j=n} a_i b_j\right) T^n.$$

1. Montrer que cela définit une structure d'anneau. On notera $k[[T]]$ cet anneau.

2. Montrer qu'un élément $\sum_{n=0}^{+\infty} a_n T^n \in k[[T]]$ est inversible si, et seulement si, $a_0 \neq 0$. Quel est l'inverse de $1 - T$?

3. En déduire que $k[[T]]$ est un anneau local d'idéal maximal (T).

4. Montrer que tout idéal de $k[[T]]$ est de la forme $\left(T^m\right)$ pour un certain entier naturel m et en déduire que $k[[T]]$ est principal. C'est donc un anneau de valuation discrète.

5. Pour tout $\mathbf{a} = \sum_{n=0}^{+\infty} a_n T^n \in k[[T]]$ non nul, on pose $v(\mathbf{a}) = \min\{n \in \mathbf{N} \ : \ a_n \neq 0\}$. Montrer que si $\mathbf{a}, \mathbf{b} \in k[[T]]$ sont non nuls, alors $v(\mathbf{ab}) = v(\mathbf{a}) + v(\mathbf{b})$ et si $\mathbf{a} + \mathbf{b} \neq 0$, alors $v(\mathbf{a} + \mathbf{b}) \geqslant \min(v(\mathbf{a}), v(\mathbf{b}))$.

6. Montrer que $k[[T]]^\times = v^{-1}(\{0\})$ et que deux éléments $\mathbf{a}, \mathbf{b} \in k[[T]]$ sont associés si, et seulement si, $v(\mathbf{a}) = v(\mathbf{b})$.

7. Soit $r \in \mathbf{N}$ et $(a_n)_{n\in\mathbf{N}}$ une suite vérifiant la relation de récurrence

$$\forall n \geqslant r, \quad a_n = \sum_{i=1}^{r} \lambda_i a_{n-i},$$

avec $\lambda_1, \ldots, \lambda_r \in k$ fixés. Supposons alors que $a_0 \neq 0$. Montrer que l'inverse de $\sum_{n=0}^{+\infty} a_n T^n$ est de la forme

$$\frac{1 - \lambda_1 T - \cdots - \lambda_r T^r}{P(T)},$$

pour un certain polynôme $P \in k[T]$ de degré au plus $r - 1$.

8. Si $F_0 = F_1 = 1$ et si pour tout $n \geqslant 2$, $F_n = F_{n-1} + F_{n-2}$, trouver une écriture de la série formelle $\sum_{n=0}^{+\infty} F_n T^n$ comme quotient de deux polynômes.

Solution.

1. C'est immédiat à partir des définitions.

2. La condition est clairement nécessaire au vu de la définition du produit. Supposons réciproquement que $a_0 \neq 0$. On construit alors l'inverse $\sum_{n\geqslant 0} b_n T^n$ de proche en proche de sorte que

$$\left(\sum_{n\geqslant 0} a_n T^n\right)\left(\sum_{n\geqslant 0} b_n T^n\right) = 1.$$

Cela impose $b_0 = a_0^{-1}$ puis $a_0 b_1 + b_0 a_1 = 0$ soit $b_1 = -\frac{a_1}{a_0^2}$ et $b_n = -\frac{1}{a_0}\sum_{i=1}^{n} a_i b_{n-i}$. On vérifie par exemple que l'inverse de $1 - T$ est $\sum_{n\geqslant 0} T^n$.

3. On a vu dans le TD III que cela équivaut au fait que l'ensemble des éléments non inversibles forment un idéal, ce qui est clairement le cas ici d'après **2.** L'idéal maximal est alors cet idéal correspondant aux éléments tels que $a_0 = 0$, autrement dit (T).

4. Soit I un idéal distinct de $k[[T]]$. On sait alors que $I \subseteq (T)$. On pose alors

$$a = \min_{\mathbf{a}\in I\setminus\{0\}} \min\{k \in \mathbf{N} \,:\, a_k \neq 0\}.$$

On a alors par définition $I \subseteq (T^a)$ et si l'on considère $\mathbf{a} \in I$ réalisant ce minimum, on peut écrire $\mathbf{a} = T^a \mathbf{a}'$ avec $a_0' \neq 0$ si bien que $\mathbf{a}' \in k[[T]]^\times$ et $(T^a) \subseteq I$. On a donc $I = (T^a)$ et tout idéal est principal.

5. C'est immédiat à partir des définitions.

6. C'est immédiat à partir des définitions et de l'exercice sur les anneaux de valuation discrète du TD III. On a notamment que $v(\mathbf{a}) = m$ si, et seulement si, $(\mathbf{a}) = (T^m)$.

7. On pose $\sum_{n=0}^{+\infty} a_n T^n$. On a

$$T^{n+r} a_{n+r} = \sum_{i=1}^{r} \lambda_i T^{n+r} a_{n+r-i}$$

soit

$$S - a_0 - a_1 T - a_2 T^2 - \cdots - a_{r-1} T^{r-1} = \lambda_1 T(S - a_0 - a_1 T - \cdots - a_{r-2} T^{r-2}) + \cdots + \lambda_r T^r S$$

et finalement

$$S(1 - \lambda_1 T - \cdots - \lambda_r T^r) = P(T)$$

pour un certain polynôme P de degré au plus $r - 1$ ce qui fournit le résultat.

8. On pose $S = \sum_{n=0}^{+\infty} F_n T^n$. On a $T^{n+2} F_{n+2} = T^{n+2} F_{n+1} + T^{n+2} F_n$ soit $S - F_0 - F_1 T = T(S - F_0) + T^2 S$ soit $S(1 - T - T^2) = 2 - T$ et finalement $S = (1 - T - T^2)^{-1}$.

EXERCICE 16.

1. Soient K et L deux corps tels que L contienne K ainsi que $P, Q \in K[X]$. Montrer que le pgcd de P et Q dans $K[X]$ est le même que le pgcd de P et Q dans $L[X]$.
Indication : On pourra commencer par le cas premier entre eux.

2. Donner un exemple de corps non commutatif et de polynôme admettant plus de racines que son degré sur ce corps.

SOLUTION.

1. On a deux anneaux de Bézout. On commence alors par traiter le cas de P et Q premiers entre eux sur L. Il existe alors deux polynômes $U, V \in K[X]$ tels que $PU + QV = 1$. Comme en particulier, $U, V \in L[X]$, on en déduit que P et Q restent premiers entre eux sur K. Réciproquement, si P et Q sont premiers entre eux sur L et si on a un facteur en commun dans $K[X]$, ce facteur est aussi dans $L[X]$, ce qui est absurde. On en déduit l'équivalence souhaitée.

À présent, si $\text{pgcd}(P, Q) = D_K$ le pgcd dans $K[X]$ et notons D_L celui dans $L[X]$. Alors, on a $P = D_K P'$ et $Q = D_K Q'$ avec P', Q' deux polynômes de $K[X]$ premiers entre eux sur K donc sur L. On a donc

$$D_L = \text{pgcd}(P, Q) = \text{pgcd}(D_K P', D_K Q') = D_K \text{pgcd}(P', Q') = D_K.$$

On peut aussi s'en convaincre en examinant de près l'algorithme d'Euclide de calcul du pgcd et en constatant qu'il est le même sur $K[X]$ ou sur $L[X]$!

2. Il suffit par exemple de considérer $X^2 + 1$ sur les quaternions $\mathbf{H}$ qui possède trois racines i, j, k.