TD4 : Anneaux noethériens et modules, anneaux de polynômes

Diego Izquierdo

Les exercices 1, 4, 6, 7 et la première question de l'exercice 11 ont été traités pendant la séance.

Exercice 1 (à préparer) : Vrai ou faux ?
Soit A un anneau.

1. Tout sous-anneau d'un anneau noethérien est noethérien.
2. Tout anneau intègre noethérien est factoriel.
3. Si A est intègre, toute famille libre maximale de A^n est de cardinal n.
4. Si A est intègre, toute famille génératrice minimale de A^n est de cardinal n.
5. Si M est un groupe abélien et M_{tor} est le sous-module de torsion de M, alors M_{tor} a un supplémentaire dans M.
6. Si A est intègre, tout sous-module d'un A-module libre est libre.
7. Il existe un $\mathbb{Z}$-module qui n'a pas de famille génératrice minimale.
8. Si $0 \to M_1 \to M_2 \to M_3 \to 0$ est une suite exacte de A-modules et M_1 et M_3 sont de type fini, alors M_2 est de type fini.
9. Pour $\alpha \in \mathbb{C}$, l'anneau $\mathbb{Z}[\alpha]$ est noethérien.
10. Si A est noethérien, un sous-A-module d'un A-module de type fini est de type fini.

Exercice 2 : Vrai ou faux ? Le retour
Soit A un anneau.

1. Tout quotient d'un anneau noethérien est noethérien.

   Indications : VRAI : Soient A un anneau et I un idéal de A. Soit J un idéal de A/I. Soit $\tilde{J} = p^{-1}(J)$ où $p : A \to A/I$ est la projection canonique. Comme A est noethérien, il existe $j_1, ..., j_r \in A$ tels que $\tilde{J} = (j_1, ..., j_r)$. On a alors $J = p(\tilde{J}) = (p(j_1), ..., p(j_r))$.
2. Tout anneau factoriel est noethérien.

   Indications : FAUX : Dans le TD3, nous avons vu que $\mathbb{Z}[(X_n)_{n\in\mathbb{N}}]$ est factoriel. Mais il n'est pas noethérien puisque l'idéal engendré par les X_n (pour $n \in \mathbb{N}$) n'est pas de type fini.
3. Si I est un idéal de type fini de A et A/I est noethérien, alors A est noethérien.

   Indications : FAUX : Prendre A la sous-$\mathbb{C}$-algèbre de $\mathbb{C}[X, Y]$ engendrée par les X^nY pour $n > 0$. D'après l'exercice 1 du TD2, A n'est pas noethérien, mais $A/XA \cong \mathbb{C}[T]$ est principal.
4. Un produit fini d'anneaux noethériens est un anneau noethérien.

Indications : VRAI : Soient $A_1, ..., A_r$ des anneaux. Soit $A = \prod_i A_i$. Soit I un idéal de A. Il existe $I_1, ..., I_r$ des idéaux de $A_1, ..., A_r$ tels que $I = \prod_i I_i$. Pour chaque I, il existe $a_{i,1}, ..., a_{i,s_i} \in A_i$ tels que $I_i = (a_{i,1}, ..., a_{i,s_i})$. L'idéal I est alors engendré par les éléments de la forme $(b_1, ..., b_r)$, avec $b_1 = 0$, ..., $b_{i-1} = 0$, $b_i = a_{i,j}$, $b_{i+1} = 0$, ..., $b_r = 0$.

5. Toute famille génératrice minimale de A^n est de cardinal au moins n.

Indications : VRAI : S'il existait une famille génératrice de A^n de cardinal au plus $n-1$, il existerait un morphisme surjectif de A-modules $f : A^{n-1} \to A^n$. Soit $(e_1, ..., e_n)$ la base canonique de A^n. Pour chaque $i \in \{1, ..., n\}$, soit $x_i \in A^{n-1}$ tel que $f(x_i) = e_i$. Soient $g : A^n = A^{n-1} \oplus A \to A^n, (x, y) \mapsto f(x)$ et $h : A^n \to A^n = A^{n-1} \oplus A, e_i \mapsto (x_i, 0)$. On vérifie aisément que $g \circ h = Id$. Donc $\det g \det h = 1$. Mais $\det h = 0$: absurde !

6. Toute famille libre maximale de A^n est une base de A^n.

Indications : FAUX : (2) est une famille libre maximale de $\mathbb{Z}$ mais n'est pas une base.

7. Toute famille génératrice minimale de A^n est une base.

Indications : FAUX : $(2, 3)$ est une famille génératrice minimale du $\mathbb{Z}$-module $\mathbb{Z}$, mais n'est pas une base.

8. Il existe un $\mathbb{Z}$-module qui n'a pas de famille libre maximale.

Indications : FAUX : Soit M un groupe abélien. Soit $\mathcal{E}$ l'ensemble des familles libres de M. Il est non vide puisqu'il contient la famille vide. On vérifie aisément que l'inclusion est un ordre inductif. Par conséquent, $\mathcal{E}$ possède un élément maximal.

9. Un $\mathbb{Z}$-module sans torsion est libre.

Indications : FAUX : Le groupe abélien $\mathbb{Q}$ est sans torsion, mais il n'est pas libre puisqu'il est divisible.

10. Si $0 \to M_1 \to M_2 \to M_3 \to 0$ est une suite exacte de A-modules et M_1 et M_3 sont libres de rang fini, alors M_2 est libre de rang $\mathrm{rg}(M_1) + \mathrm{rg}(M_3)$.

Indications : VRAI : On note $f : M_1 \to M_2$ et $g : M_2 \to M_3$ les morphismes apparaissant dans la suite exacte. Soit $(e_1, ..., e_r)$ une base de M_3. Soient $x_1, ..., x_r$ des éléments de M_2 tels que $g(x_i) = e_i$ pour chaque i. Soit $h : M_3 \to M_2$ le morphisme tel que $h(e_i) = x_i$ pour chaque i. On vérifie alors que $M_1 \oplus M_3 \to M_2, (x, y) \mapsto f(x) + h(y)$ est un isomorphisme de A-modules, ce qui achève la preuve.

11. Si $A[X]$ est noethérien, alors A est noethérien.

Indications : VRAI : A est un quotient de $A[X]$.

Exercice 3 : Noethérianité et factorialité

Soit A un anneau intègre noethérien. Montrer que tout élément non nul de A s'écrit sous la forme $up_1...p_n$ avec $u \in A^\times$ et p_i irréductible pour chaque i. L'anneau A est-il forcément factoriel ?

Indications : Supposons que A possède un élément qui ne s'écrit pas sous la forme désirée. Soit $\mathcal{E}$ la famille des idéaux principaux engendrés par un élément de A qui ne s'écrit pas sous la forme désirée. Par noethérianité de A, la famille $\mathcal{E}$ possède un élément maximal I pour l'inclusion. Soit x un générateur de I. Comme $I \in \mathcal{E}$, x n'est ni inversible ni irréductible. On peut donc écrire $x = yz$ avec y et z non inversibles. Par maximalité de I, y et z s'écrivent sous la forme $up_1...p_n$ avec $u \in A^\times$ et p_i irréductible pour chaque i. Il en est donc de même pour x : absurde ! Donc tout élément non nul de A s'écrit sous la forme $up_1...p_n$ avec $u \in A^\times$ et p_i irréductible pour chaque i. Par contre, A n'est pas forcément factoriel : par exemple, $A = \mathbb{C}[T^2, T^3] = \mathbb{C}[X, Y]/(X^2 - Y^3)$ est noethérien non factoriel.

Exercice 4 : Idéaux premiers minimaux

Soit A un anneau noethérien.

1. En raisonnant par l'absurde, montrer que, pour tout idéal I de A, il existe des idéaux premiers $\mathfrak{p}_i$ vérifiant $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{n_I} \subseteq I$.
2. Montrer que l'on peut exiger $I \subseteq \mathfrak{p}_i$ pour tout $1 \leq i \leq n_I$ dans la question précédente.
3. En déduire qu'il existe un nombre fini d'idéaux premiers minimaux.

Exercice 5 : Une caractérisation des anneaux noethériens

Soient A un anneau, I un idéal de A et a un élément de A. Montrer que si $I + (a)$ et $\{x \in A \mid ax \in I\}$ sont des idéaux de type fini de A, alors I est de type fini. En déduire que A est noethérien si, et seulement si, tous ses idéaux premiers sont de type fini.

Indications : On écrit $I + (a) = (f_1, ..., f_r)$ et $\{x \in A \mid ax \in I\} = (g_1, ..., g_s)$. Pour $i \in \{1, ..., r\}$, on écrit $f_i = h_i + ak_i$ avec $h_i \in I$ et $k_i \in A$. On vérifie alors aisément que $I = (h_1, ..., h_r, ag_1, ..., ag_s)$.
Supposons maintenant que tout idéal premier de A est de type fini. Soit $\mathcal{E}$ la famille constituée des idéaux de A qui ne sont pas de type fini, et supposons que $\mathcal{E}$ soit non vide. L'inclusion est un ordre inductif sur $\mathcal{E}$. Donc, d'après le lemme de Zorn, $\mathcal{E}$ possède un élément maximal I_0. Par hypothèse, I_0 n'est pas premier, donc il existe $a, b \in A$ tels que $a \notin I_0$, $b \notin I_0$ et $ab \in I_0$. Par maximalité $I_0+(a)$ et $I_0+(b)$ sont de type fini. Donc $\{x \in A \mid ax \in I_0\}$ et $\{x \in A \mid bx \in I_0\}$ ne sont pas de type fini, et toujour par maximalité, $\{x \in A \mid ax \in I_0\} = \{x \in A \mid bx \in I_0\} = I_0$. Mais alors $A = \{x \in A \mid abx \in I_0\} = I_0$: absurde ! Donc $\mathcal{E}$ est vide.

Exercice 6 : Modules noethériens

Soit A un anneau. Soient M, N et P trois A-modules. Supposons qu'il existe un morphisme injectif de A-modules $i : M \to N$ et un morphisme surjectif de A-modules $p : N \to P$ tels que $p \circ i = 0$. Montrer que N est noethérien si, et seulement si, M, P et $\mathrm{Ker}(p)/\mathrm{Im}(i)$ sont noethériens.

Exercice 7 : Endomorphismes surjectifs d'un module noethérien

Considérons A un anneau et M un A-module noethérien. Soit $u : M \to M$ un morphisme de A-modules. Montrer qu'il existe $n \in \mathbb{N}$ tel que $\mathrm{Ker}(u^n) \cap \mathrm{Im}(u^n) = 0$. En déduire que, si u est surjectif, alors u est un isomorphisme. Ce résultat subsiste-t'il si M n'est pas supposé noethérien ?

Exercice 8 : Modules noethériens et polynômes
Soient A un anneau et M un A-module. Montrer que $M[X]$ est un $A[X]$-module noethérien si, et seulement si, M est un A-module noethérien.

Indications : Supposons M noethérien. Soit N un sous-A[X]-module de M[X]. Montrons qu'il est de type fini. Soit

$N_n = \{m \in M / \exists P \in N : deg(P) = n$ et m est le coefficient dominant de $P\} \cup \{0\}$.

Les N_n sont des A-modules et la suite $(N_n)_n$ est croissante. Comme M est noethérien, la suite des $(N_n)_n$ est stationnaire, disons à partir de n_0 et les modules N_n sont engendrés par un nombre fini d'éléments, les $(b_{n,k})_{1 \leq k \leq k_n}$. Pour chaque paire (n,k), notons $P_{n,k} \in N$ un polynôme de degré n dont le coefficient dominant est $b_{n,k}$. Nous allons montrer que N est engendré par les $(P_{n,k})_{1 \leq n \leq n_0, 1 \leq k \leq k_n}$. Soit N_0 le sous-A[X]-module de $M[X]$ engendré par ces éléments. Soit $P \in N$ de degré d. Montrons par récurrence sur d que $P \in N_0$. Notons m le coefficient dominant de P. On a $m \in N_d$. Si $d \leq n_0$, alors $m = \sum_k a_k b_{d,k}$ pour certains $a_k \in A$ et donc $Q = P - \sum_k a_k P_{d,k} \in N$ est de degré strictement inférieur à d Par hypothèse de récurrence, on déduit que $Q \in N_0$, ce qui montre que $P \in N_0$. Si $d > n_0$, alors $m \in N_d = N_{n_0}$ et il existe des $a_k \in A$ tels que $Q = P - X^{d-n_0} \sum_k a_k P_{n_0,k} \in N$ est encore de degré strictement inférieur à d. On conclue comme précédemment.

Exercice 9 : L'anneau $\hat{\mathbb{Z}}$
Pour n et m deux entiers naturels non nuls tels que $n|m$, on note $\pi_{m,n}$ la projection naturelle $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. On pose :

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \{(x_n)_n \in \prod_n \mathbb{Z}/n\mathbb{Z} \mid \forall (n,m) \in (\mathbb{N}^*)^2, n|m \Rightarrow \pi_{m,n}(x_m) = x_n\}.$$

En notant $\mathcal{P}$ l'ensemble des nombres premiers, montrer que $\hat{\mathbb{Z}} \cong \prod_{p \in \mathcal{P}} \mathbb{Z}_p$.

Indications : On définit $\varphi : \hat{\mathbb{Z}} \to \prod_p \mathbb{Z}_p, (x_n)_n \mapsto ((x_{p^m})_m)_p$. Montrons que c'est un isomorphisme d'anneaux. Soit $x = (x_n) \in \mathrm{Ker}(\varphi)$. Pour tout premier p, pour tout $m > 0$, on a $x_{p^m} = 0$. Soit n un entier naturel quelconque, et écrivons sa décomposition en produit de facteurs premiers : $n = \prod_{i=1}^r p_i^{m_i}$. L'image de x_n par le morphisme $\mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^r \mathbb{Z}/p_i^{m_i}\mathbb{Z}$ est $(x_{p_1^{m_1}}, ..., x_{p_r^{m_r}}) = 0$. Mais ce morphisme est un isomorphisme d'après le lemme chinois. Donc $x_n = 0$ et φ est injectif.
Soit maintenant $y = ((y_{p,m})_m)_p \in \prod_p \mathbb{Z}_p$. Soit $n \in \mathbb{N}$ non nul et écrivons sa décomposition en produit de facteurs premiers : $n = \prod_{i=1}^r p_i^{m_i}$. Soit x_n l'image réciproque de $(y_{p_1,m_1}, ..., y_{p_r,m_r})$ par l'isomorphisme $\mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^r \mathbb{Z}/p_i^{m_i}\mathbb{Z}$ donné par le lemme chinois. On vérifie alors aisément que la suite (x_n) est dans $\hat{\mathbb{Z}}$ et que $\varphi((x_n)) = y$. On en déduit que φ est surjectif.

Exercice 10 : Une question de convergence
Pour quels nombres premiers p la suite (10^n) converge-t'elle dans $\mathbb{Z}_p$?

> **Indications :** Si $p \in \{2,5\}$, alors $v_p(10^n) \to +\infty$ quand $n \to +\infty$, donc 10^n tend vers 0 dans $\mathbb{Z}_p$.
>
> Si $p \notin \{2,3,5\}$, la suite $(\overline{10}^n)$ à valeurs dans $\mathbb{Z}/p\mathbb{Z}$ est périodique non constante : donc la suite (10^n) diverge dans $\mathbb{Z}_p$.
>
> Si $p = 3$, la suite $(\overline{10}^n)$ à valeurs dans $\mathbb{Z}/27\mathbb{Z}$ est périodique non constante : donc la suite (10^n) diverge dans $\mathbb{Z}_3$.

Exercice 11 : Entiers p-adiques et équations
Soit p un nombre premier.

1. Rappeler pourquoi $\mathbb{Z}_p$ est compact.

2. Soit $m > 0$. Soit $f \in \mathbb{Z}[X_1, ..., X_m]$. Montrer que l'équation $f(x_1, ..., x_m) = 0$ a des solutions dans $\mathbb{Z}_p$ si, et seulement si, elle a des solutions dans $\mathbb{Z}/p^r\mathbb{Z}$ pour tout r.

Exercice 12 : Lemme de Hensel et applications

1. Soient A un anneau et I un idéal de A.

(i) Soit n entier naturel non nul. Soient $f \in A[X]$ et $x \in A$ tels que $f(x) \equiv 0 \mod I^n$ et $f'(x) \in (A/I)^\times$. Montrer qu'il existe $y \in A$ tel que $y \equiv x \mod I^n$ et $f(y) \equiv 0 \mod I^{n+1}$. Montrer que si $z \in A$ est tel que $z \equiv x \mod I^n$ et $f(z) \equiv 0 \mod I^{n+1}$, alors $z \equiv y \mod I^{n+1}$.

(ii) Soient $f \in A[X]$ et $x \in A$ tels que $f(x) \equiv 0 \mod I$ et $f'(x) \in (A/I)^\times$. Déduire de la question précédente qu'il existe un unique $y \in \varprojlim_n A/I^n$ tel que son image dans A/I coïncide avec celle de x et $f(y) = 0$.

2. Est-ce que 14 possède une racine carrée dans $\mathbb{Z}_5$? Dans $\mathbb{Z}_7$? Dans $\mathbb{Z}_{11}$?

3. Soit p un nombre premier. En utilisant le lemme de Hensel, montrer que $\mathbb{Z}_p$ possède $p-1$ racines $p-1$-ièmes de l'unité.

4. Montrer qu'il existe $f(T) \in \mathbb{Z}[[T]]$ tel que $f(T)^5 + f(T) + T = 0$. En écrivant $f(T) = \sum_{n \geq 0} a_n T^n$, calculer a_n pour $n \leq 6$.

Exercice 13 (difficile) : Complétion et produit
Soient A un anneau et I un idéal. Montrer que, si A/I est un produit non trivial de deux anneaux, il en est de même pour $\hat{A} = \varprojlim_n A/I^n$.

Indications : Soit $n \in \mathbb{N} \setminus \{0\}$. Soit $e \in A$ tel que $e^2 \equiv e \mod I^n$. On note $f = e^2 - e$ et on calcule alors $(3e^2 - 2e^3)^2 - 3e^2 + 2e^3 \equiv -8e^3 - 12e^2 f + 11e^2 + 20ef - 3e - 3f \equiv 0 \mod I^{n+1}$. De plus, $3e^2 - 2e^3 \equiv 3e - 2e \equiv e \mod I^n$. On a donc construit $e' \in A$ tel que $e' \equiv e \mod I^n$ et $e'^2 \equiv e' \mod I^{n+1}$.
Soit maintenant $e_1 \in A$ non congru à 0 ou 1 modulo I tel que $e^2 \equiv e \mod I$. Par récurrence, on construit $e_n \in A$ tel que $e_n^2 \equiv e_n \mod I^n$ et $e_{n+1} \equiv e_n \mod I^n$. On en déduit que l'élément (e_n) de $\varprojlim_n A/I^n$ est un idempotent différent de 0 et 1, ce qui achève la preuve.

Exercice 14 : L'anneau des entiers p-adiques

1. Rappeler pourquoi $\mathbb{Z}_p$ est un anneau intègre.

Soit $\mathbb{Q}_p$ le corps des fractions de $\mathbb{Z}_p$.

2. Pour $x = (x_n)_n \in \mathbb{Z}_p$, on pose $v_p(x) = \max\{n \in \mathbb{N} / x_n = 0\}$. Montrer que v_p étend la valuation p-adique sur $\mathbb{Z}$. Vérifier que la topologie de $\mathbb{Z}_p$ est induite par la distance :

$$d_p(x, y) = p^{-v_p(x-y)}.$$

3. Montrer que la fonction $v_p : \mathbb{Z}_p \to \mathbb{N}$ s'étend en un morphisme de groupes surjectif $v_p : \mathbb{Q}_p \to \mathbb{Z}$. Montrer que $\mathbb{Z}_p = \{x \in \mathbb{Q}_p / v_p(x) \geq 0\}$ et que $\mathbb{Z}_p^\times = \mathrm{Ker}(v_p)$.

4. En déduire que l'anneau $\mathbb{Z}_p$ est principal. Quels sont ses idéaux ? Montrer que, pour chaque $x \in \mathbb{Z}_p$, on a $\mathbb{Z}_p/(x) \cong \mathbb{Z}/p^{v_p(x)}\mathbb{Z}$.

5. Quels sont les idéaux premiers (resp. maximaux) de $\mathbb{Z}_p$?

6. La surjection $\pi : \mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ induit par restriction un morphisme de groupes surjectif $\pi : \mathbb{Z}_p^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$. Montrer qu'il possède une section, c'est-à-dire qu'il existe un morphisme de groupes $s : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ tel que $\pi \circ s = Id$.

7. On pose $s(0) = 0$. Montrer que la fonction :

$$\phi : (\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}} \to \mathbb{Z}_p, (x_n)_n \mapsto \sum_n s(x_n)p^n$$

est une bijection. S'agit-il d'un isomorphisme d'anneaux ?

8. Il est intéressant de comprendre quelle structure d'anneau il faut mettre sur $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}}$ pour que ϕ soit un isomorphisme. C'est la théorie des vecteurs de Witt qui y répond, mais elle dépasse très largement le cadre de ce cours.

Exercice 15 : Séries formelles

Soit k un corps. Pour $x \in k[[T]]$ et $y \in k[[T]]$, on pose $v(x) = \max\{n \in \mathbb{N} / x \in (T^n)\}$ et $d(x, y) = e^{-v(x-y)}$. Montrer que d définit une distance sur $k[[T]]$ et que $k[[T]]$ est alors un anneau qui s'identifie au complété de $k[T]$

pour la distance d. Quand $k[[T]]$ est-il compact ?

Indications : On vérifie aisément que, pour $x, y \in k[[T]]$, on a :

$$v(x+y) \geq \min\{v(x), v(y)\}.$$

On en déduit que, pour $x, y, z \in k[[T]]$:

$$d(x,z) \leq \max\{d(x,y), d(y,z)\}.$$

Comme $d(x,y) = 0$ si, et seulement si, $x = y$, la fonction d est bien une distance sur $k[[T]]$.

Soit $f(T) = \sum_n a_n T^n \in k[[T]]$. Alors :

$$\sum_{n \leq k} a_n T^n \to f(T)$$

dans $k[[T]]$ lorsque $k \to +\infty$. Cela montre que $k[T]$ est dense dans $k[[T]]$.

Considérons maintenant une suite de Cauchy (f_i) dans $k[[T]]$. On écrit :

$$f_i = \sum_n a_n^{(i)} T^n.$$

Fixons un entier $n_0 \geq 0$. Comme la suite (f_n) est de Cauchy, il existe $N > 0$ tel que, pour tout $k \geq 0$, on a $v(f_N - f_{N+k}) \geq n_0 + 1$. On remarque alors que, pour tout $k \geq 0$, on a $a_{n_0}^{(N+k)} = a_{n_0}^N$. On pose $a_n = a_{n_0}^N$ et $f = \sum_n a_n T^n \in k[[T]]$. On vérifie alors aisément que la suite (f_n) converge vers f. Donc $k[[T]]$ est complet : c'est bien le complété de $k[T]$.

Supposons $k[[T]]$. On remarque que k est fermé dans $k[[T]]$ (c'est le complémentaire de la boule ouverte de centre 0 et de rayon 1). Donc k est compact et discret : il est fini.

Réciproquement, supposons k fini. L'anneau topologique $k[[T]]$ s'identifie à $\varprojlim_n k[T]/(T^n)$. Chaque $k[T]/(T^n)$ est fini discret donc compact. Le théorème de Tychonov montre alors que $k[[T]]$ est compact.

Exercice 16 : Séries et rayon de convergence

Soit p un nombre premier. Soit (a_n) une suite à valeurs dans $\mathbb{Q}_p$. Montrer que la série $\sum_{n \geq 0} a_n$ converge si, et seulement si, la suite (a_n) converge vers 0. Dire pour quels $x \in \mathbb{Q}_p$ les séries suivantes convergent :

1. $\sum_{n \geq 0} \frac{x^n}{n!}$.
2. $\sum_{n \geq 0} n x^n$.
3. $\sum_{n \geq 0} n! x^n$.
4. $\sum_{n \geq 0} 10^n x^n$.

Exercice 17 : Structure de $\mathbb{Z}_p^\times$

Soit p un nombre premier impair. On note $U^{(1)} = 1 + p\mathbb{Z}_p$.

1. Montrer que le groupe des racines de l'unité dans $\mathbb{Z}_p$ est cyclique d'ordre $p-1$. En déduire que, si p et l sont deux nombres premiers impairs distincts, alors $\mathbb{Q}_p$ et $\mathbb{Q}_l$ ne sont pas isomorphes.

> **Indications :** L'anneau $\mathbb{Z}_p$ étant intègre, il possède au plus m racines m-ièmes de l'unité pour chaque m. Pour tout entier naturel n, on a un isomorphisme :
>
> $$f_n : \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z} \to (\mathbb{Z}/p^n\mathbb{Z})^\times,$$
>
> qui envoie $(0,1)$ sur $1+p$. Par conséquent, les racines de l'unité dans $\mathbb{Z}_p$ sont chacune d'ordre divisant $(p-1)p^s$ pour un certain s. Soit $x = (x_n)$ une racine p-ième de l'unité dans $\mathbb{Z}_p$. Alors pour chaque $n > 0$, il existe $k_n \in \mathbb{N}$ tel que $x_n = (1+p)^{k_n}$ et $p^{n-2}|k_n$. De plus, comme $x \in \mathbb{Z}_p$, on a $k_{n+1} \equiv k_n \mod p^{n-1}$, donc $p^{n-1}|k_n$, et $x_n = 1$. On en déduit que la seule racine p-ième de l'unité dans $\mathbb{Z}_p$ est 1, et donc que toute racine de l'unité dans $\mathbb{Z}_p$ est d'ordre divisant $p-1$. Pour conclure, il suffit d'invoquer la question 3 de l'exercice 12.

2. Montrer que :

$$\mathbb{Z}_p^\times = \mu_{p-1} \times U^{(1)},$$

où μ_{p-1} désigne le sous-groupe des racines $(p-1)$-ièmes de l'unité. A quoi est isomorphe μ_{p-1} ? Le groupe $U^{(1)}$ peut-il avoir des éléments de torsion ?

> **Indications :** Dans la question 6 de l'exercice 14, on a vu que l'on a une suite exacte scindée :
>
> $$1 \to U^{(1)} \to \mathbb{Z}_p^\times \to (\mathbb{Z}/p\mathbb{Z})^\times) \to 1.$$
>
> Cela montre que $\mathbb{Z}_p^\times = \mu_{p-1} \times U^{(1)}$, où $\mu_{p-1} \cong \mathbb{Z}/(p-1)\mathbb{Z}$.
>
> Si x est un élément de torsion de $U^{(1)}$, c'est une racine de l'unité : d'après la question 1, c'est une racine d'ordre $(p-1)$, donc $x \in \mu_{p-1}$: absurde ! Cela prouve que $U^{(1)}$ n'a pas d'éléments de torsion.

3. On considère les séries :

$$\exp(x) = \sum_{n \geq 0} \frac{x^n}{n!},$$

$$\log(1+x) = \sum_{n \geq 1} (-1)^{n+1} \frac{x^n}{n}.$$

Montrer que exp : $p\mathbb{Z}_p \to U^{(1)}$ et log : $U^{(1)} \to p\mathbb{Z}_p$ définissent des isomorphismes de groupes continus, inverses l'un de l'autre.

> **Indications :**

Exercice 18 : Condition de Mittag-Leffler

Soient $(A_n)_{n\in\mathbb{N}}$ et $(B_n)_{n\in\mathbb{N}}$ deux systèmes projectifs de groupes abéliens indexés par $\mathbb{N}$. On note $f_n : A_{n+1} \to A_n$ et $g_n : B_{n+1} \to B_n$ les morphismes

de transition. Un morphisme de systèmes projectifs $h : (A_n) \to (B_n)$ est la donnée d'un morphisme de groupes $h_n : A_n \to B_n$ pour chaque n de sorte que $h_n \circ f_n = g_n \circ h_{n+1}$.

1. Montrer qu'un morphisme de systèmes projectifs $h : (A_n) \to (B_n)$ induit un morphisme de groupes abéliens $h : \varprojlim_n A_n \to \varprojlim_n B_n$.

Indications : Le morphisme h induit un morphisme de groupes abéliens :

$$h : \prod_n A_n \to \prod_n B_n.$$

De plus, pour $x = (x_n)_n \in \varprojlim_n A_n$, on a :

$$g_{n-1}(h_n(x_n)) = h_{n-1}(f_{n-1}(x_n)) = h_{n-1}(x_{n-1}),$$

ce qui montre que $h(x) \in \varprojlim_n B_n$. Donc h induit un morphisme :

$$h : \varprojlim_n A_n \to \varprojlim_n B_n.$$

2. On dit qu'une suite de morphismes de systèmes projectifs $0 \to (A_n) \to (B_n) \to (C_n) \to 0$ est exacte si, pour chaque n, la suite $0 \to A_n \to B_n \to C_n \to 0$ est exacte. Montrer qu'une suite exacte de systèmes projectifs $0 \to (A_n) \to (B_n) \to (C_n) \to 0$ induit une suite exacte de groupes abéliens $0 \to \varprojlim_n A_n \to \varprojlim_n B_n \to \varprojlim_n C_n$. Montrer que le dernier morphisme n'est pas nécessairement surjectif.

Indications : Notons $h : (A_n) \to (B_n)$ et $k : (B_n) \to (C_n)$ les morphismes de systèmes projectifs. Soit $(a_n)_n \in \varprojlim A_n$ tel que $h((a_n)_n) = 0$. Alors pour chaque n, on a $h_n(a_n) = 0$. Comme h_n est injectif, cela prouve que $a_n = 0$ pour chaque n. Autrement dit, $(a_n)_n$ est nul et $h : \varprojlim_n A_n \to \varprojlim_n B_n$ est injectif.

Par ailleurs, comme pour chaque n la composée $k_n \circ h_n$ est nulle, la composée $k \circ h : \varprojlim_n A_n \to \varprojlim_n C_n$ l'est aussi. Donc $\mathrm{Im}(h) \subseteq \mathrm{Ker}(k)$.

Réciproquement, soit $(b_n)_n \in \varprojlim_n B_n$ tel que $k((b_n)_n) = 0$. Alors pour chaque n, on a $k_n(b_n) = 0$. Cela montre qu'il existe $a_n \in A_n$ tel que $h_n(a_n) = b_n$. On calcule alors :

$$h_{n-1}(f_{n-1}(a_n)) = g_{n-1}(h_n(a_n)) = g_{n-1}(b_n) = b_{n-1})h_{n-1}(a_{n-1}).$$

Comme h_{n-1} est injectif, cela montre que $f_{n-1}(a_n) = a_{n-1}$, et donc que $(a_n)_n \in \varprojlim_n A_n$. On a bien sûr $h((a_n)_n) = (b_n)_n$, et donc Donc $\mathrm{Im}(h) = \mathrm{Ker}(k)$. On a bien montré que la suite $0 \to \varprojlim_n A_n \to \varprojlim_n B_n \to \varprojlim_n C_n$ est exacte.

3. Soit $0 \to (A_n) \to (B_n) \to (C_n) \to 0$ une suite exacte de systèmes projectifs. On note $f_n : A_{n+1} \to A_n$ les morphismes de transition. On suppose que f_n est surjectif pour n assez grand. Montrer que la suite $0 \to \varprojlim_n A_n \to \varprojlim_n B_n \to \varprojlim_n C_n \to 0$ est exacte.

Indications : Voir le lemme 3.1 du chapitre 1 du livre *Algebraic Geometry and Arithmetic Curves* de Qing Liu.

4. Soit $0 \to (A_n) \to (B_n) \to (C_n) \to 0$ une suite exacte de systèmes projectifs. On note $f_n : A_{n+1} \to A_n$ les morphismes de transition. On pose $f_{m,n} = f_n \circ f_{n+1} \circ ... \circ f_{m-1}$ pour $m \geq n$. On suppose que le système (A_n) vérifie la condition de Mittag-Leffler : pour chaque $n \geq 0$, la suite $(f_{m,n}(A_m))_{m\in\mathbb{N}}$ stationne. Montrer que la suite $0 \to \varprojlim_n A_n \to \varprojlim_n B_n \to \varprojlim_n C_n \to 0$ est exacte.

Indications : Suivre les indications de l'exercice 3.15 du chapitre 1 du livre *Algebraic Geometry and Arithmetic Curves* de Qing Liu. On pourra aussi regarder le Stacks Project : http ://stacks.math.columbia.edu/tag/0594 (ici la preuve est faite dans le cas plus général où la limite projective est indexée par un ensemble dénombrable ordonné).

Exercice 19 : Complétion et noethérianité

1. Soit G un groupe abélien topologique. La complétion de G est un groupe abélien topologique séparé complet K muni d'un morphisme continu $\phi : G \to K$ vérifiant la propriété universelle suivante : pour chaque morphisme continu h de G dans un groupe abélien topologique séparé complet K', il existe un unique morphisme continu $h' : K \to K'$ tel que $h = h' \circ \phi$.

On suppose que G est muni d'une suite décroissante $(G_n)_{n\in\mathbb{N}}$ de sous-groupes qui forme une base de voisinages ouverts de 0. On note $\hat{G} = \varprojlim_n G/G_n$, et :

$$\hat{G}_n = \{(a_m)_m \in \hat{G} | a_m = 0 \text{ pour } m \leq n\}.$$

Les sous-groupes $\hat{G}_n$ de $\hat{G}$ définissent une structure de groupe topologique sur $\hat{G}$ telle que les $\hat{G}_n$ forment une base de voisinages ouverts de 0. Soit $\pi : G \to \hat{G}$ le morphisme naturel. Montrer que $\hat{G}$ muni de π est la complétion de G, puis que π induit un isomorphisme $G/G_n \to \hat{G}/\hat{G}_n$ pour chaque entier n.

Indications : Voir la proposition 3.2 du chapitre 1 du livre *Algebraic Geometry and Arithmetic Curves* de Qing Liu.

Si A est un anneau et I un idéal, la complétion I-adique de A est $\varprojlim_n A/I^n$: c'est donc la complétion de A au sens de la question précédente à condition de munir A de la structure de groupe topologique pour laquelle les I^n forment une base de voisinages ouverts de 0.

2. Soit A un anneau. Soient $B = A[T_1, ..., T_n]$ et $J = (T_1, ..., T_n) \subseteq B$. Montrer que la complétion J-adique de B est $\hat{B} = A[[T_1, ..., T_n]]$.

Indications : Voir l'exemple 3.6 du chapitre 1 du livre *Algebraic Geometry and Arithmetic Curves* de Qing Liu.

3. Montrer que, si A est noethérien, alors $A[[T_1, ..., T_n]]$ l'est aussi.

Indications : Voir la proposition 3.7 du chapitre 1 du livre *Algebraic Geometry and Arithmetic Curves* de Qing Liu.

4. Soient M et N des groupes abéliens munis respectivement de filtrations (ie de suites décroissantes de sous-groupes) $(M_n)_{n\in\mathbb{N}}$ et $(N_n)_{n\in\mathbb{N}}$. Soit $\phi : M \to N$ un morphisme de groupes tel que, pour un certain $n_0 \geq 0$, on ait $N = \phi(N)+N_n$ et $N_n = \phi(M_n)+N_{n+1}$ pour tout $n \geq n_0$. Montrer que le morphisme naturel $\varprojlim_n M/M_n \to \varprojlim_n N/N_n$ est surjectif. On pourra utiliser la question 3 de l'exercice 20.

Indications : Voir le lemme 3.3 du chapitre 1 du livre *Algebraic Geometry and Arithmetic Curves* de Qing Liu.

5. Soient A un anneau noethérien et I un idéal de A. Déduire des questions précédentes que $\hat{A} = \varprojlim_n A/I^n$ est noethérien.

Indications : Voir le corollaire 3.8 du chapitre 1 du livre *Algebraic Geometry and Arithmetic Curves* de Qing Liu.