Anneaux et arithmétique (ANAR)
TD 3 : Polynômes et séries formelles

Salim Rostam

1 Polynômes

Exercice 1. Soit A un anneau commutatif unitaire. Les anneaux $A[X]$ et $A^{(\mathbb{N})}$ sont-ils isomorphes ?

Exercice 2. Soit k un corps et soit $P \in k[X]$.

1) Montrer que si P est irréductible de degré $\neq 1$ alors P n'a pas de racine sur k.
2) Donner une condition suffisante sur P pour que la réciproque soit vraie.
3) Montrer que $X^3 + X^2 + 1$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[X]$.

Exercice 3. Décomposer le polynôme $X^3 - X$ de $\mathbb{Z}/6\mathbb{Z}[X]$ en un produit de facteurs linéaires et déterminer ses racines.

Exercice 4. Soit k un corps et soit $n \in \mathbb{N}^*$.

1) Soit d un diviseur de n. Montrer que $X^d - 1$ divise $X^n - 1$ dans $k[X]$.
2) Soit $d \geq 1$ et r le reste de la division euclidienne de n par d. Montrer que $X^r - 1$ est le reste de la division euclidienne de $X^n - 1$ par $X^d - 1$.

Exercice 5. Soient $k \subseteq k'$ deux corps et $P, Q \in k[X]$. On suppose que $P \mid Q$ dans $k'[X]$. A-t-on $P \mid Q$ dans $k[X]$?

Exercice 6. Soit A un anneau commutatif intègre unitaire. Que dire de l'idéal (X) de $A[X, Y]$?

Exercice 7. Soit A commutatif unitaire.

1) Soient $a \in A^\times$ et $b \in A$. Montrer qu'il existe un unique automorphisme de l'anneau $A[X]$ qui laisse invariant les éléments de A et envoie X sur $aX + b$.
2) On suppose A intègre. Montrer que les automorphismes de $A[X]$ qui laissent invariant les éléments de A sont du type précédent.

Exercice 8. Soit A commutatif unitaire. Montrer que $P(X)-X$ divise $P\Big(P(X)\Big)-X$ dans $A[X]$. *Indication : on pourra poser* $Y = P(X)$.

Exercice 9. Soit k un corps.

1) Montrer que les k-algèbres $k[X] \otimes k[Y]$ et $k[X, Y]$ sont isomorphes.
2) Plus généralement, montrer que si A est une k-algèbre alors $A \otimes k[X] \simeq A[X]$.

Exercice 10. Soit A un anneau commutatif unitaire. Montrer que $\mathrm{M}_n\Big(A[X_1, \ldots, X_r]\Big) \simeq \mathrm{M}_n(A)[X_1, \ldots, X_r]$.

Exercice 11. Soit A commutatif unitaire intègre. Montrer que $A[X_1, \ldots, X_n]^\times = A^\times$.

Exercice 12. Soit k un corps et G un sous-groupe fini de $k^\times$. Le but de cet exercice est de montrer que G est cyclique. Soit n l'ordre de G.

1) Montrer que si n est premier alors G est cyclique.

On suppose maintenant que $n = ab$ avec $1 < a, b$ premiers entre eux. On considère l'application $f : G \to G$ donnée par $x \mapsto x^a$.

2) Justifier que f est bien à valeurs dans G.
3) Montrer que f est un morphisme de groupes.
4) Montrer que $\#\ker f \leq a$ et $\#\mathrm{im}\, f \leq b$.
5) Montrer que $\#\ker f \#\mathrm{im}\, f = n$.
6) En déduire par récurrence que G possède un élément d'ordre a et un élément d'ordre b.
7) En déduire que G est cyclique.

Exercice 13. Soit A un anneau commutatif sans élément nilpotent non nul (*i.e.* $\mathrm{Nil}(A) = (0)$ (cf. TD2) ; on dit que A est *réduit*).

1) Montrer qu'un anneau intègre satisfait à l'hypothèse.
2) Donner un exemple d'un anneau comme dans l'énoncé mais non intègre.
3) Montrer que $P \in A[X]$ est un diviseur de 0 si et seulement si il existe $a \neq 0 \in A$ tel que $aP = 0$.

Exercice 14. Soit A commutatif unitaire intègre et $P, Q \in A[X]$. Montre que si Q est unitaire, il existe un unique couple $(R, S) \in A[X]$ avec $\deg S < \deg Q$ tel que $P = QR + S$.

Exercice 15. Soit k un corps et $n \geq 2$. En faisant une division euclidienne à $X^n \in k[X]$, déterminer la puissance n-ième de la matrice $\left(\begin{smallmatrix} 5 & -4 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{M}_2(k)$.

Exercice 16. Soit k un corps. On regarde l'anneau $A = \mathrm{End}_k\big(k[X]\big)$ des endomorphismes du k-espace vectoriel $k[X]$.

1) On considère l'endomorphisme $d : P \mapsto P'$. Admet-il un inverse à gauche ? À droite ?
2) Même question avec $m : P \mapsto XP$.

Exercice 17 (Matrice universelle)**.** Soit $n \geq 1$. On considère l'anneau $A = \mathbb{Z}[X_{ij}]_{1\leq i,j\leq n}$.

1) Rappeler pourquoi A est intègre.

On considère k le corps des fractions de A et on considère la matrice $M = (X_{ij})_{1\leq i,j\leq n} \in \mathrm{M}_n(k)$.

2) a) Montrer que $\det M \neq 0$. *Indication* : qu'implique $\det M = 0$?
   b) Soit $N = (Y_{ij})_{1\leq i,j\leq n}$. Montrer que $\chi_{MN} = \chi_{NM}$ dans $\mathbb{Z}[(X_{ij}), (Y_{ij})][T]$.
   c) En déduire que si B est un anneau commutatif unitaire et $M, N \in \mathrm{M}_n(B)$ alors $\chi_{MN} = \chi_{NM}$ dans $B[T]$.
3) a) Montrer que les valeurs propres de M (calculée dans une clôture algébrique de k) sont deux à deux distinctes. *On rappelle qu'il existe une application* $\mathrm{disc} : A[T] \to A$ *telle que* $\mathrm{disc}(P) = 0_A$ *si et seulement si* $P \in A[T]$ *possède une racine multiple dans* $\overline{k}$.
   b) En déduire que $\chi_M(M) = 0$ (sans utiliser le théorème de Cayley–Hamilton).
   c) Soit B un anneau commutatif unitaire. En déduire le théorème de Cayley–Hamilton dans $\mathrm{M}_n(B)$.

Exercice 18 (Polynômes homogènes)**.** Soit k un corps. Pour $d \geq 0$, un polynôme *homogène de degré* d est un polynôme $P \in E_d \coloneqq \mathrm{vect}_k\Big(X_1^{n_1} \cdots X_r^{n_r} : \sum_i n_i = d\Big)$.

1) Démontrer que $k[X_1, \ldots, X_r] = \oplus_{d\geq 0} E_d$ en tant que k-espaces vectoriels.
2) Déterminer $\dim_k E_d$.

Exercice 19 (Théorème fondamental des polynômes symétriques)**.** Soit k un corps. On dit que $P \in k[X_1, \ldots, X_n]$ est *symétrique* si pour tout $\sigma \in \mathfrak{S}_n$ on a $P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n)$. Pour $d \in \{0, \ldots, n\}$, on définit le *polynôme symétrique élémentaire de degré* d :

$$\sigma_d(X_1, \ldots, X_n) \coloneqq \sum_{1\leq i_1<\cdots<i_d\leq n} X_{i_1} \cdots X_{i_d} \in k[X_1, \ldots, X_n].$$

1) Expliciter $\sigma_1, \sigma_2, \sigma_3$.
2) Montrer que σ_d est symétrique.
3) Montrer que σ_d est homogène de degré d (voir Exercice 18).

4) Montrer que

$$\prod_{i=1}^{n}(T - X_i) = \sum_{d=0}^{n}(-1)^{n-d}\sigma_{n-d}(X_1, \ldots, X_n)T^d.$$

À un monôme $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, on associe le n-uplet $\alpha = (\alpha_1, \ldots, \alpha_n)$. Soit $P \in k[X_1, \ldots, X_n]$ un polynôme symétrique. On veut montrer que P est de la forme $Q(\sigma_1, \ldots, \sigma_n)$ pour $Q \in k[\Sigma_1, \ldots, \Sigma_n]$.

5) Soit α le plus grand n-uplet pour l'ordre lexicographique tel que X^α apparait dans P. Montrer que α est décroissant.

Soit $a \in k^\times$ le coefficient de P devant X^α. On considère le polynôme

$$\widetilde{P} \coloneqq P - a\sigma_1^{\alpha_1 - \alpha_2} \cdots \sigma_{n-1}^{\alpha_{n-1} - \alpha_n}\sigma_n^{\alpha_n}.$$

6) Montrer que si P est homogène de degré d alors $\widetilde{P}$ reste homogène de degré d.

7) Montrer que $\widetilde{P} \in k[X_1, \ldots, X_n]$ est un polynôme symétrique.

8) Soit β le plus grand n-uplet pour l'ordre lexicographique tel que X^β apparait dans $\widetilde{P}$. Montrer que $\beta < \alpha$ pour l'ordre lexicographique.

9) En déduire par récurrence le théorème. *Remarque : on peut montrer que le polynôme Q est unique.*

10) Soit $n \geq 3$. On considère le polynôme symétrique $P_n \in k[X_1, \ldots, X_n]$ engendré par le monôme $X_1^2X_2^2X_3$ (c'est-à-dire $P_n = \sum_{\sigma \in \mathfrak{S}_n} X_{\sigma(1)}^2 X_{\sigma(2)}^2 X_{\sigma(3)}$). Soit $Q_n \in k[\Sigma_1, \ldots, \Sigma_n]$ tel que $P_n = Q_n(\sigma_1, \ldots, \sigma_n)$.
    a) Expliciter P_3 et déterminer Q_3.
    b) Expliciter P_4 et déterminer Q_4.
    c) Si $n \geq 5$, montrer que $Q_5 = \Sigma_2\Sigma_3 - 3\Sigma_1\Sigma_4 + 5\Sigma_5$.

Exercice 20 (Théorème de Kronecker)**.** Soit $P \in \mathbb{Z}[X]$ unitaire dont les racines complexes z vérifient $|z| \leq 1$. On veut montrer que les racines non nulles de P sont des racines de l'unité.

1) Montrer que l'on peut supposer $X \nmid P$.

Notons $P = \prod_{i=1}^n (X - \alpha_i)$ pour $\alpha_i \in \mathbb{C}$ et pour tout $m \geq 1$, on pose $P_m \coloneqq \prod_{i=1}^n (X - \alpha_i^m)$.

2) Donner une borne indépendante de m pour les coefficients de P_m.

3) À l'aide du théorème fondamental des polynômes symétriques (Exercice 19), montrer que $P_m \in \mathbb{Z}[X]$.

4) Conclure.

2 Séries formelles

Exercice 21. Soit A un anneau commutatif unitaire intègre. Les anneaux $A[[X]]$ et $A^{\mathbb{N}}$ sont-ils isomorphes ?

Exercice 22. Soit A un anneau commutatif unitaire.

1) Quels sont les éléments inversibles de $A[[X]]$? Donner un procédé d'inversion.
2) Quel est l'inverse de $1 - X$ dans $A[[X]]$?

Exercice 23. Soit A un anneau commutatif unitaire.

1) Comparer les anneaux $A[X][[Y]]$ et $A[[Y]][X]$.
2) Comparer les anneaux $A[[X]][[Y]]$ et $A[[Y]][[X]]$.

Exercice 24. Soit k un corps de caractéristique nulle.

1) On considère $\exp X \coloneqq \sum_{n\geq 0} \frac{1}{n!} X^n \in k[[X]]$. Montrer que $(\exp X)' = \exp X$.

Soit $A \in k[[X]]$. On s'intéresse à l'équation différentielle $F' = AF$ d'inconnue $F \in k[[X]]$.

1) Montrer qu'il existe un unique $\tilde{A} \in k[[X]]$ avec $\tilde{A}(0) = 0$ tel que $(\tilde{A})' = A$.
2) Montrer que $\exp(\tilde{A})$ est solution de l'équation différentielle (on utilisera les règles de dérivation usuelles pour la composition).
3) Si F est une solution, montrer que $\exp(-\tilde{A})F$ est solution de $G' = 0$.
4) En déduire l'ensemble des solutions de $F' = AF$.
5) En déduire que pour tout $\lambda \in k$, l'équation différentielle admet une unique solution F vérifiant $F(0) = \lambda$.

Exercice 25. Soit k un corps.

1) Déterminer les idéaux de $k[[X]]$. *Indication* : quels sont les inversibles de $k[[X]]$?
2) En déduire que $k[[X]]$ est local (cf. TD 2 : possède un unique idéal maximal).

On considère l'application $v : k[[X]] \setminus \{0\} \to \mathbb{N}$ donnée par la valuation (X-adique) : étant donné $F \in k[[X]]$, l'entier $v(P)$ est le plus grand entier $n \geq 0$ tel qu'il existe $G \in k[[X]]$ avec $F = X^n G$. On pose par convention $v(0) \coloneqq +\infty$.

3) Montrer que $v(F + G) \geq \min\Big(v(F), v(G)\Big)$.
4) Montrer que $d : (F, G) \mapsto 2^{-v(F-G)}$ est une distance (*ultra-métrique*) sur $k[[X]]$.

On munit maintenant $k[[X]]$ de la topologie définie par la distance d.

5) Soit $F = \sum_{n\geq 0} a_n X^n$.
   a) Montrer que F est la limite des polynômes $\sum_{n=0}^{N} a_n X^n$ quand $N \to +\infty$.

b) Réciproquement, montrer que si $(F_M)_{M\geq 0}$ est une suite de séries formelles qui converge vers F alors pour tout $N \geq 0$, les termes de degré $\leq N$ des F_M coïncident pour M assez grand.

6) Montrer que $k[[X]]$ est complet.

7) Montrer que $k[[X]]$ est le complété de $k[X]$.

8) On suppose dans cette question que $k = \mathbb{R}$.
   a) Existe-t-il une norme qui rende complet $\mathbb{R}[X]$?
   b) Existe-t-il une distance qui rende complet $\mathbb{R}[X]$?

9) On suppose k de caractéristique nulle. A-t-on $\lim_{n\to+\infty}\left(1+\frac{1}{n}X\right)^n = \exp X$?

10) Montrer que $k[[X]]$ est compact si et seulement si k est fini.

Exercice 26. Soit k un corps.

1) Soient $P, Q \in k[[X]]$. La composition $P \circ Q$ a-t-elle toujours un sens ?

Soit $Q \in k[[X]]$ avec $v(Q) \geq 1$ (notation de l'Exercice 25). On définit l'application $\phi_Q : k[[X]] \to k[[X]]$ par $P \mapsto P \circ Q$.

2) Montrer que ϕ_Q est un endomorphisme de l'algèbre $k[[X]]$.

3) Montrer que ϕ_Q est injectif.

4) Monter que ϕ_Q est surjectif si et seulement si $v(Q) = 1$.

5) Montrer que l'on obtient ainsi tous les automorphismes de l'algèbre $k[[X]]$.

Exercice 27 (Sommes de Newton)**.** Soit k un corps. Pour $d \geq 1$ on pose

$$N_d \coloneqq \sum_{i=1}^{n} X_i^d \in k[X_1, \ldots, X_n].$$

1) Montrer que N_d est symétrique et homogène de degré d.

L'objectif est de montrer les *formules de Newton* :

$$N_d = \begin{cases} \sum_{k=1}^{d-1}(-1)^{k-1}\sigma_k N_{d-k} + (-1)^{d-1} d\sigma_d, & \text{si } d \leq n, \\ \sum_{k=1}^{n}(-1)^{k-1}\sigma_k N_{d-k}, & \text{si } d \geq n, \end{cases}$$

où les σ_k sont les polynômes symétriques élémentaires de l'Exercice 19. On considère

$$\sigma(T) \coloneqq \prod_{i=1}^{n}(1 - X_i T).$$

2) Montrer que la fonction génératrice des sommes de Newton :

$$N(T) \coloneqq \sum_{d\geq 1} N_d T^d,$$

vérifie

$$N(T) = \sum_{i=1}^{n} \frac{X_i T}{1 - X_i T}.$$

3) En déduire que
$$N(T) = \frac{-T\sigma'(T)}{\sigma(T)}.$$
4) En déduire l'expression des sommes de Newton en fonction des polynômes symétriques élémentaires.
5) En déduire que si k est de caractéristique 0, tout polynôme symétrique peut s'écrire comme un polynôme en les sommes de Newton.

Exercice 28 (Produits infinis et partitions)**.** 1) Soit k un corps. Pour chaque $m \geq 1$, soit $F_m \in k[[X]]$ tel que $F_m - 1_k \in (X)$. Montrer que si pour tout $n \geq 1$ l'ensemble $\{m : v(F_m - 1_k) \leq n\}$ est fini alors on peut donner un sens à $\prod_{m=1}^{+\infty} F_m$.
2) Soit $p(n)$ le nombre de *partitions* de l'entier $n \geq 1$, c'est-à-dire, le nombre de suites $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_h > 0)$ décroissantes (au sens large) d'entiers positifs de somme n.
   a) Déterminer $p(n)$ pour $n \in \{1, \ldots, 5\}$.
   b) Montrer que
$$p(n) = \#\left\{\alpha_1, \ldots, \alpha_n \in \mathbb{N} : \sum_{k=0}^{n} \alpha_k k = n\right\}.$$
   c) Montrer que dans $\mathbb{Q}[[X]]$ on a
$$\sum_{n\geq 0} p(n)X^n = \prod_{k\geq 1} \frac{1}{1-X^k}.$$
3) Soit $p_i(n)$ (resp. $p_d(n)$) le nombre de partitions de n en entiers impairs (resp. en parts distinctes), c'est-à-dire avec tous les λ_k impairs (resp. distincts).
   a) Montrer que
$$\sum_{n\geq 0} p_i(n)X^n = \prod_{k\geq 0} \frac{1}{1-X^{2k+1}}, \qquad \sum_{n\geq 0} p_d(n)X^n = \prod_{k\geq 0}(1+X^k).$$
   b) En déduire que $p_i = p_d$.

Exercice 29. On définit
$$\ln(1+X) \coloneqq \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} X^n \in \mathbb{Q}[[X]].$$
1) Montrer que $\Big(\ln(1+X)\Big)' = \frac{1}{1+X}$ (au sens de l'Exercice 22).
2) Montrer que $\exp\Big(\ln(1+X)\Big) = 1+X$ et $\ln\Big(\exp(X)\Big) = X$ en :
   a) utilisant ces résultats connus pour les fonctions réelles correspondantes ;
   b) utilisant le résultat de l'Exercice 24.

Exercice 30 (Formule d'inversion de Pascal)**.** Soit k un corps de caractéristique nulle et soient $(a_n), (b_n) \in k^{\mathbb{N}}$. On considère les séries génératrices exponentielles associées :

$$F \coloneqq \sum_{n\geq 0} \frac{a_n}{n!} X^n \in k[[X]],$$
$$G \coloneqq \sum_{n\geq 0} \frac{b_n}{n!} X^n \in k[[X]].$$

1) Déterminer la suite (c_n) d'éléments de k telle que $FG = \sum_{n\geq 0} \frac{c_n}{n!} X^n \in k[[X]]$.
2) On suppose que $b_n = \sum_{k=0}^{n} \binom{n}{k} a_k$ pour tout $n \geq 0$. Montrer que $a_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} b_k$.

Exercice 31 (Nombres de Bell)**.** Soit B_n le nombre de partitions de $\{1, \ldots, n\}$.

1) Montrer que $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$. *Indication* : Comment construire par récurrence une partition de $\{1, \ldots, n+1\}$?
2) En déduire que la série génératrice exponentielle $F \coloneqq \sum_{n\geq 0} \frac{B_n}{n!} X^n \in \mathbb{Q}[[X]]$ des B_n vérifie $F' = \exp(X)F$.
3) En déduire que $F = \exp\Big(\exp(X) - 1\Big)$.

Exercice 32 (Produit tensoriel)**.** Soit k un corps.

1) Montrer que le morphisme naturel de k-algèbres $\iota : k[[X]] \otimes k[[Y]] \to k[[X, Y]]$ est injectif.
2) On considère un élément de l'image de ι, que l'on écrit $\sum_{n\geq 0} F_n(X) Y^n$ avec $F_n \in k[[X]]$. Montrer que le k-espace vectoriel engendré par les F_n est un sous-k-espace vectoriel de $k[[X]]$ de dimension finie.
3) En déduire que l'image de ι :
   a) est strictement incluse dans $k[[X, Y]]$;
   b) n'est pas un anneau local. *Indication* : on pourra trouver deux éléments non inversibles de somme 1_k.