Travaux Dirigés – Exercices. Série IV

Semaine IV-V-VI. 08/10/07 – 28/10/07

A– Composée d'un polynôme et d'une fraction rationnelle

Soit K un corps. Soient $P \in K[X]$ et $F \in K(X)$ tels que $P(F(X)) \in K[X]$. Montrer que P est constant ou que $F \in K[X]$.

B– Distinction entre polynômes et fonctions polynomiales

Soit A un anneau commutatif. Posons $P = X(1-X) \in A[X]$.

1. Donner un exemple où on a $P(a) = 0$ ($a \in A$).
2. Peut-on trouver un tel exemple avec A de cardinal 2, 3, 4 ?
3. Peut-on trouver un tel exemple avec A infini ?
4. Peut-on trouver un tel exemple avec A infini et intègre ?

C– L'anneau $A[X]$ n'est pas principal quand A n'est pas un corps.

Soit A un anneau commutatif. Si A est un corps, on sait que $A[X]$ est un anneau principal. Supposons que A n'est pas un corps. Soit $a \in A$ un élément non inversible et non nul.

1. Montrer que l'idéal engendré par a est distinct de A.
2. Soit I l'idéal de $A[X]$ engendré par a et X. Montrer que cet idéal n'est pas principal.

D– Automorphismes de $K[X]$.

Soit A un anneau commutatif intègre. Notons K le corps des fractions de A.

1. Supposons que A est un sous-anneau d'un anneau B. Démontrer que l'ensemble des automorphismes de B qui sont l'identité quand on les restreint à A constitue un groupe pour la composition des applications.
2. Soient $a \in A^*$ et $b \in A$. Montrer que l'application $A[X] \to A[X]$ qui à P associe $P(aX+b)$ est un automorphisme de $A[X]$ qui est l'identité quand on le restreint à A.
3. Soit ϕ un automorphisme de $A[X]$ qui est l'identité sur A. Montrer qu'il existe $a \in A^*$ et $b \in A$ tels que $\phi(P) = P(aX+b)$.
4. En déduire que le groupe des automorphismes de $A[X]$ qui sont l'identité sur A est en bijection avec $A^* \times A$. Indiquer comment s'exprime la composition des automorphismes via cette bijection. En déduire une loi de groupe sur $A^* \times A$. (Ne peut-on la retrouver grâce aux matrices 2×2 ?)
5. Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$. Montrer que l'application $K(X) \to K(X)$ qui à F associe $F((aX+b)/(cX+d))$ est un automorphisme de $K(X)$, qui est l'identité sur K.
6. Montrer que le groupe des automorphismes du corps $K(X)$ qui sont l'identité sur K est isomorphe au groupe $\mathrm{GL}_2(K)$.

E– Irréductibilité des polynômes de $\mathbf{Z}[X]$

Soit $P = aX^3 + bX^2 + cX + d \in \mathbf{Z}[X]$.

1. Montrer que si P est réductible, il admet une racine $u/v \in \mathbf{Q}$ (où u et v sont des entiers premiers entre eux). Montrer qu'alors $u|d$ et $v|a$.
2. En déduire un algorithme pour déterminer si P est irréductible.
3. Montrer que le polynôme $X^3 + 274X^2 + 721X + 13$ est irréductible sur $\mathbf{Q}$.

F– Diverses méthodes pour établir l'irréductibilité

1. Donner la décomposition en produit de polynômes irréductibles de $X^5 - 1 \in \mathbf{F}_2[X]$.
2. Peut-on établir l'irréductibilité de $X^5 - 7 \in \mathbf{Q}[X]$ en examinant sa réduction modulo 2 ?
3. Soit $P \in \mathbf{F}_{11}[X]$ un polynôme irréductible de degré 2. Montrer que $k = \mathbf{F}_{11}[X]/(P)$ est un corps à 121 éléments, puis que tout élément non nul de k est d'ordre divisant 120 dans k^*.
4. Montrer que 7 n'est pas une puissance cinquième dans k.
5. En déduire que $X^5 - 7 \in \mathbf{Q}[X]$ est irréductible.

G– Un polynôme irréductible de $\mathbf{Z}[X]$ dont toutes les réductions modulo p sont réductibles

1. Soit p un nombre premier $\neq 2$. Montrer que $p^2 - 1$ est divisible par 8. Soit k un corps à p^2 éléments (contenant donc un sous-corps à p éléments $\mathbf{F}_p$). Combien k^* a-t-il d'éléments d'ordre 8 ? Combien le polynôme $X^4 + 1 \in k[X]$ a-t-il de racines dans k ?
2. Montrer que le polynôme $X^4 + 1 \in \mathbf{F}_p[X]$ est irréductible si, et seulement si, il a une racine dans un corps à p^2 éléments. En déduire que le polynôme $X^4 + 1 \in \mathbf{F}_p[X]$ est réductible pour tout nombre premier p.
3. Montrer que $X^4 + 1 \in \mathbf{Q}[X]$ est irréductible.
4. Montrer que le polynôme $(X^2 - 2)(X^2 - 3)(X^2 - 6) \in \mathbf{Q}[X]$ ne possède aucune racine dans $\mathbf{Q}$ et que sa réduction modulo p admet une racine dans $\mathbf{F}_p$ pour tout nombre premier p.

H– Irréductibilité sur $\mathbf{Q}(i)$

Montrer que le polynôme $X^3 + X + 1$ est irréductible sur le corps $\mathbf{Q}(i)$.

I– Irréductibilité dans $\mathbf{Q}[X, Y]$

1. Rappeler quels sont les polynômes irréductibles de $\mathbf{Q}[X, Y]$.
2. Montrer que le polynôme $X^5 + XY^3 + Y(Y + 1)$ est irréductible dans $\mathbf{Q}[X, Y]$.

J– Irréductibilité en fonction d'un paramètre

1. À quelle condition sur le nombre rationnel a, le polynôme $X^4 - a$ est-il irréductible ?
2. À quelle condition sur le nombre entier a, le polynôme $X^4 - aX - 1$ est-il irréductible ?

K– Polynômes de $\mathbf{Q}[X]$ prenant des valeurs entières en les entiers

Considérons l'ensemble E des polynômes $P \in \mathbf{Q}[X]$ tels que $P(n) \in \mathbf{Z}$ pour tout $n \in \mathbf{Z}$. Posons, pour n entier ≥ 1, $B_n(X) = X(X-1)\cdots(X-n+1)/n! \in \mathbf{Q}[X]$.

1. Montrer que $B_n \in E$ (n entier ≥ 0).
2. Montrer que E est un $\mathbf{Z}$-module.
3. Quels sont les éléments de E de degré 1, de degré 2, de degré 3 ?
4. Montrer que pour tout $Q \in \mathbf{Q}[X]$ de degré d, il existe un unique $(c_0, c_1, ..., c_d) \in \mathbf{Q}^n$ tel que $Q = c_0B_0 + ... + c_nB_n$. Donner le lien entre c_0, $c_1 ... c_n$ et $Q(0)$, $Q(1)$,$\cdots$,$Q(n)$.
5. Montrer que $Q \in E$ si, et seulement si, on a c_0, c_1, $\cdots$, $c_n \in \mathbf{Z}$.
6. Soit $P \in \mathbf{Q}[X]$ de degré d. Montrer que $P \in E$ si, et seulement si, $P(0)$, $P(1)$,$\cdots$,$P(n)$ sont tous entiers. En déduire que $P \in E$ si et seulement P prend des valeurs entières en $n+1$ entiers consécutifs.
7. Soit $P \in \mathbf{Q}[X]$. Montrer que $P \in E$ si, et seulement si, P prend des valeurs entières en un nombre infini d'entiers consécutifs.

L- Polynômes de Bernoulli

Soit $x \in \mathbf{R}$. Considérons la fonction f_x de classe $\mathcal{C}^\infty$ qui au nombre réel t associe $te^{tx}/(e^t-1)$. (On pourrait prendre des variables complexes ou mieux identifier les séries sans se préoccuper de la convergence.)

1. Montrer que le développement en série entière de f_x en 0 est de la forme $f_x(t) = \sum_{k=0}^{\infty} B_k(x)t^k/k!$, où B_k est un polynôme de degré k de $\mathbf{Q}[X]$ (c'est le k-ème *polynôme de Bernoulli*).
2. Calculer B_0, B_1, B_2.
3. Soient k et n des entiers > 0. Montrer la formule $B_k(X) = n^{k-1}\sum_{a=0}^{n-1} B_k((X+a)/n)$ (on pourra traduire cette formule en une formule sur f_x).
4. Soit k un entier > 0. Montrer la formule $B_k(X+1) - B_k(X) = kX^{k-1}$ (le polynôme B_k est la "primitive discrète" de kX^{k-1}).
5. Soient k et n des entiers > 0. Donner une formule pour $\sum_{i=1}^{n} i^{k-1}$ à l'aide de B_k. Application à $k = 3$.

M- Polynômes alternés

Soit K un corps de caractéristique $\neq 2$. Soit n un entier > 0. Posons $A = K[T_1, ..., T_n]$. Considérons la matrice $(T_i^j)_{1 \leq i,j \leq n} \in \mathrm{M}_n(A)$. Notons V son déterminant (c'est un *déterminant de Vandermonde*). Soit $P \in A$. On dit que P est un *polynôme alterné* si l'action du groupe symétrique $\mathcal{S}_n$ sur P est donnée par la formule $\sigma(P) = \mathrm{sgn}(\sigma)P$.

1. Soient i et $j \in \{1, ..., n\}$ deux entiers distincts. Notons $\phi_{i,j}$ l'homorphisme d'anneaux $A \to A$ tel que $\phi_{i,j}(T_k) = T_k$ si $k \neq j$ et $\phi_{i,j}(T_j) = T_i$. Montrer que le noyau de $\phi_{i,j}$ est l'idéal principal engendré par $T_i - T_j$. Montrer que tout polynôme alterné est dans le noyau de $\phi_{i,j}$.
2. Montrer que $T_i - T_j$ divise V dans A ($1 \leq i, j \leq n$, $i \neq j$). En raisonnant sur les degrés, montrer que $V = \prod_{j<i}(T_i - T_j)$.

3. Soient i, i', j et $j' \in \{1, ..., n\}$ tels que les paires $\{i, j\}$ et $\{i', j'\}$ soient distinctes. Montrer qu'on a les égalités d'idéaux de A : $(T_j - T_i) \cap (T_{j'} - T_{i'}) = (T_j - T_i)(T_{j'} - T_{i'})$. En déduire l'égalité d'idéaux de A : $(V) = \cap_{i<j}(T_i - T_j)$.
4. Montrer P est alterné si, et seulement si, il existe un polynôme symétrique $Q \in A$ tel que $P = QV$.
5. Montrer que P est invariant sous l'action du groupe alterné $\mathcal{A}_n$ si, et seulement si, il existe des polynômes symétriques Q et $R \in A$ tels que $P = QV + R$.
6. Cette dernière propriété est-elle encore vérifiée si la caractéristique de K est 2 ?

N- Polynômes caractéristiques

Soit K un corps commutatif. Soit n un entier > 0. Considérons le corps $L = K((A_{i,j})_{1\leq i,j\leq n}, (B_{i,j})_{1\leq i,j\leq n})$ (corps des fractions rationnelles en $2n^2$ indéterminées).

1. On considère les matrices $A = (A_{i,j})_{1\leq i,u\leq n}$ et $B = (B_{i,j})_{1\leq i,u\leq n}$ dans $\mathrm{M}_n(L)$. Donner leurs déterminants et montrer que ces derniers sont non nuls. Les matrices A et B sont-elles inversibles dans $\mathrm{M}_n(L)$?
2. Soient M et N deux matrices inversibles de $\mathrm{M}_n(L)$. Montrer que les matrices $XI_n - MN$ et $XI_n - NM \in \mathrm{M}_n[L(X)]$ sont conjuguées. En déduire que le polynôme caractéristique de MN est égal au polynôme caractéristique de NM.
3. Montrer que le polynôme caractéristique de AB appartient à $K[(A_{i,j})_{1\leq i,u\leq n}, (B_{i,j})_{1\leq i,u\leq n}, X]$, puis que le polynôme caractéristique de AB est égal au polynôme caractéristique de BA.
4. Soit $A_0 = (\alpha_{i,j})_{1\leq i,j\leq n}$ et $B_0 = (\beta_{i,j})_{1\leq i,j\leq n} \in \mathrm{M}_n(K)$. Montrer que les polynômes caractéristiques de A_0B_0 et B_0A_0 sont obtenus en évaluant les polynômes caractéristiques de AB et BA respectivement. En déduire que les polynômes caractéristiques de A_0B_0 et B_0A_0 sont égaux.

O- Discriminants Soit K un corps. Soit k un sous-corps de K. On suppose que K est un k-espace vectoriel de dimension finie n. Soit $x \in K$. On note M_x la multiplication par x dans K. C'est une application k-linéaire. On pose $N(x) = \det(M_x)$.

1. Soit P le polynôme minimal de x. Montrer que le degré de P divise n. On note m ce degré et on pose $n = pm$.
2. Notons a_0 le terme constant de P. Montrer que $N(x) = (-1)^n a_0^p$. Plus généralement, on montrera que le polynôme caractéristique de M_x est P^p.
3. Supposons que $m = n$. Soit L un corps contenant K comme sous-corps tel que $P(X) = \prod_{i=1}^n (X - x_i)$ dans $L[X]$. Montrer que $N(x) = \prod_{i=1}^n x_i$.
4. Soit $y \in K$. Montrer que $y = Q(x)$ avec $Q \in k[X]$ et en déduire que $N(y) = \prod_{i=1}^n Q(x_i)$. On pose

$$D(P) = \prod_{i\neq j}(x_i - x_j).$$

5. Montrer que $D(P) \in k$.
6. Soit $y = P'(x)$. Montrer que $D(P) = N(y)$.

7. On suppose désormais que $P(X) = X^n + aX + b$ avec a, $b \in k$. Calculer x en fonction de y et en déduire le polynôme minimal de y.

8. Montrer que
$$D(P) = n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n.$$

P- Résolution par radicaux des polynômes du 3-ème degré

Soit K un corps de caractéristique différente de 2 et 3. Considérons le polynôme $P = X^3+pX+q \in K[X]$. Supposons-le scindé et notons α, β et γ ses racines. On se propose de déterminer ces racines en fonctions de p et q. On suppose que K contient une racine cubique primitive de l'unité j.

1. Soit $Q \in K[X]$ de degré 3. Montrer qu'il existe $a \in K^*$ et $b \in K$ tel que $Q(aX + b)$ ait un coefficient du second degré nul.

2. Posons $R_j(X_1, X_2, X_3) = (X_1+jX_2+j^2X_3)^3 \in K[X_1, X_2, X_3]$. Montrer que l'orbite de R_j sous l'action du groupe symétrique $\mathcal{S}_3$ contient deux éléments : R_j et un autre élément qu'on notera R_{j^2}.

3. Montrer que les polynômes $R_j+R_{j^2}$ et $R_jR_{j^2}$ sont symétriques. Les exprimer en fonction des polynômes symétriques élémentaires.

4. Posons $u = R_j(\alpha, \beta, \gamma) \in K$ et $v = R_{j^2}(\alpha, \beta, \gamma) \in K$. Exprimer $u + v$ et uv en fonction de p et q.

5. Exprimer α, β et γ en fonction de u et v.

Q- Résolution par radicaux des polynômes du 4-ème degré

Soit K un corps de caractéristique différente de 2 et 3. Considérons le polynôme $P = X^4+aX^2+bX+c \in K[X]$. On le suppose scindé et on note α_1, α_2, α_3 et α_4 ses racines. On se propose de déterminer ces racines en fonction de a, b et c.

1. On considère $X_1X_2 + X_3X_4 \in K[X_1, X_2, X_3, X_4]$. Montrer que l'orbite de ce polynôme sous l'action du groupe symétrique $\mathcal{S}_4$ contient trois éléments notés U, V et W.

2. Montrer que les coefficients en X du polynôme $R(X) = (X-U)(X-V)(X-W) \in K[X_1, X_2, X_3, X_4][X]$ sont symétriques en X_1, X_2, X_3 et X_4. Exprimer ces coefficients en fonction des polynômes symétriques élémentaires.

3. Exprimer α_1, α_2, α_3 et α_4 en fonction de $U(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, $V(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ et $W(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.

4. Conclure à l'aide de l'exercice précédent.

R- Polynômes symétriques et polynômes symétriques élémentaires

Soit K un corps.

1. Montrer que le polynôme $(X_1 + X_2 - X_3 - X_4)(X_1 + X_3 - X_2 - X_4)(X_1 + X_4 - X_2 - X_3) \in K[X_1, X_2, X_3, X_4]$ est symétrique et l'exprimer en fonction des polynômes symétriques élémentaires.

2. Soient x, y, $z \in K$ tels que $x + y + z = 1$, $x^2 + y^2 + z^2 = 2$ et $x^3 + y^3 + z^3 = 3$. Calculer $x^4 + y^4 + z^4$.

S- Le théorème *abc*

Soit K_0 un corps de caractéristique 0. Soient P, Q et $R \in K_0[X]$ des polynômes scindés, non constants et deux à deux premiers entre eux tels que

$$P + Q = R.$$

Notons $z_0(PQR)$ le nombre de zéros distincts de $PQR \in K_0[X]$.

1. Les polynômes P, Q et R ont-ils des zéros communs ?
2. En posant dans $K_0(X)$, $F = P/R$ et $G = Q/R$, démontrer qu'on a $F' + G' = 0$, puis que $Q/P = -\frac{F'/F}{G'/G}$.
3. On pose $P = a\prod_{i\in I}(X - a_i)^{n_i}$, $Q = b\prod_{j\in J}(X - b_j)^{m_j}$ et $R = c\prod_{k\in K}(X - c_k)^{l_k}$, où a, b, $c \in K_0^*$ et où les familles finies $(a_i)_{i\in I}$, $(b_j)_{j\in J}$, $(c_k)_{k\in K}$ décrivent des élément distincts de K_0 et les familles $(n_i)_{i\in I}$, $(m_j)_{j\in J}$, $(l_k)_{k\in K}$ décrivent des entiers ≥ 1. Calculer P'/P, Q'/Q et R'/R. En déduire F'/F et G'/G.
4. En posant alors $N = \prod_{i\in I}(X - a_i)\prod_{j\in J}(X - b_j)\prod_{k\in K}(X - c_k)$, montrer que NF'/F et NG'/G sont des polynômes de degrés $< z_0(PQR)$.
5. En déduire que les degrés de P, Q et R sont majorés strictement par $z_0(PQR)$.
6. En déduire que si U, V, $W \in \mathbf{C}[X]$ sont non constants, premiers entre eux et vérifient $U^n + V^n = W^n$, on a $n \leq 2$.

T- Polynôme sans facteur carré

Soit K un corps. Soit $P \in K[X]$. On dit que P est *sans facteur carré* si la décomposition de P en produit de polynômes irréductibles ne comporte que des facteurs distincts. Montrer que c'est le cas si, et seulement si, le discriminant de P est nul. Si P est donné sous la forme $a_0 + a_1X + ... + a_nX^n$, est-il plus commode d'examiner la factorisation de P ou de calculer le discriminant ? Y a-t-il une méthode analogue pour montrer qu'un nombre entier est sans facteur carré ?