

Feuille 5

Résultant, Discriminant, Polynômes symétriques

1. Soit K un corps. Soient $P, Q \in K[X]$ unitaires.
 - 1.a. Notons R le reste de la division euclidienne de P par Q . Montrer que $\text{Res}(Q, P) = \text{Res}(Q, R)$.
 - 1.b. Soit $T \in K[X]$ de degré t . Montrer que $\text{Res}(P \circ T, Q \circ T) = \text{Res}(P, Q)^t$. Calculer $\text{Res}(X^6 - 1, X^9 + 1)$.
 - 1.c. Soient a et b deux éléments d'une extension algébrique L de K . Notons A et B les polynômes minimaux respectifs de a et b sur K . Montrer que le polynôme minimal de $a+b$ est un facteur de $\text{Res}_Y(A(X-Y), B(Y))$.
 - 1.d. Soit a une racine dans \mathbf{C} de $X^3 + X + 1$ et b une racine primitive 8-ème de l'unité dans \mathbf{C} . Calculer le polynôme minimal de $a + b$.
2. Soit K un corps. Soit $P \in K[X]$ un polynôme de degré n et de coefficient dominant a_n . Le *discriminant* Δ_P de P est par définition la quantité $(-1)^{n(n-1)/2} \text{Res}(P, P')/a_n$.
 - 2.a. Calculer le discriminant des polynômes $aX^2 + bX + c$ et $X^3 + aX + b$.
 - 2.b. Montrer que le discriminant du polynôme $X^n - 1$ est $(-1)^{(n-1)(n-2)/2} n^n$.
 - 2.c. Si P est scindé de racines $\alpha_1, \alpha_2, \dots, \alpha_n$, montrer que $\Delta_P = a_n^{2n-2} \prod_{i < j} (\alpha_i - \alpha_j)^2$. En déduire que Δ_P est nul si et seulement si P admet des racines multiples.
 - 2.d. Montrer que Δ_P est un polynôme à coefficients dans K en a_0, a_1, \dots, a_n , et donc un polynôme symétrique en $\alpha_1, \alpha_2, \dots, \alpha_n$. Montrer que c'est le carré d'un polynôme alterné en $\alpha_1, \alpha_2, \dots, \alpha_n$.
 - 2.e. Soit k un entier ≥ 1 . Montrer que $\Delta_{P(X^k)} = -(-1)^{n^2 k(k+1)/2} k^{kn} a_n^{k-1} \Delta_P^k P(0)^{k-1}$.
 - 2.f. Soit $Q \in K[X]$ unitaire. Supposons P unitaire. Montrer que $\Delta_{PQ} = \Delta_P \Delta_Q \text{Res}(P, Q)^2$.
 - 2.g. Montrer qu'on a, pour $P(X) = X^n + aX + b$, $\Delta_P = (-1)^{n(n-1)/2} (n^n b^{n-1} + (-1)^{n-1} (n-1)^{n-1} a^n)$.
 - 2.h. Montrer que le nombre premier $p \neq 2$ (resp. $p = 2$) divise Δ_{Φ_n} si et seulement si $p|n$ (resp. $4|n$).
 - 2.i. Soit p un nombre premier ≥ 1 . Déterminer le discriminant du polynôme cyclotomique Φ_p .
 - 2.j. Si p ne divise pas n (resp. $p|n$), montrer que $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$ (resp. $\Phi_{pn}(X) = \Phi_n(X^p)$).
 - 2.k. Soit m un entier > 2 premier à n . Montrer que $\text{Res}(\Phi_n, \Phi_m) = 1$.
 - 2.l. Montrer que, si $n > 2$, le discriminant de Φ_n est $(-1)^{\phi(n)/2} n^{\phi(n)} / \prod_{p|n} p^{\phi(n)/(p-1)}$ (p premier).
3. Soit K un corps. Soit n un entier ≥ 1 . Notons $K[X]_n$ le K -espace vectoriel des polynômes nul ou de degré $\leq n$. Les matrices 2×2 à coefficients dans K et de déterminant 1 forment un groupe pour la multiplication noté $\text{SL}_2(K)$. Ce groupe est engendré par l'ensemble $\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} / x \in K \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} / x \in K \right\}$.
 - 3.a. Montrer que $\text{SL}_2(K)$ opère à droite sur $K[X]_n$ par $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot P(X) = (cX + d)^n P((aX + b)/(cX + d))$.
 - 3.b. Montrer que pour tout $g \in \text{SL}_2(K)$, on a $\Delta_{g \cdot P} = \Delta_P$ (On pourra le montrer pour les générateurs).
4. Soit K un corps. Soit k un sous-corps de K tel que K est un k -espace vectoriel de dimension n . Soit $x \in K$. On note $M_x : K \rightarrow K$ la multiplication par x . C'est une application k -linéaire. On pose $N(x) = \det(M_x)$.
 - 4.a. Soit P le polynôme minimal de x sur k . Montrer que son degré, noté m , divise n . On pose $n = pm$.
 - 4.b. 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 .
 - 4.c. Supposons que $m = n$. Soit L un corps de décomposition de P 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.d. Soit $y \in K$. Montrer que $y = Q(x)$ avec $Q \in k[X]$ et en déduire que $N(y) = \prod_{i=1}^n Q(x_i)$.
 - 4.e. On pose $D(P) = \prod_{i \neq j} (x_i - x_j)$. Montrer que $D(P) \in k$. Soit $y = P'(x)$. Montrer que $D(P) = N(y)$.
5. Soit K un corps. Soient P et $Q \in K[X, Y]$ premiers entre eux et de degrés d et e respectivement.
 - 5.a. Montrer que le résultant $\text{Res}_Y(P, Q)$ est un polynôme en X de degré $\leq de$.
 - 5.b. En déduire que la courbe plane d'équation $P(x, y) = Q(x, y) = 0$ a au plus de points dans K^2 .
 - 5.c. Posons $P = X^2 - XY + Y^2 - 1$ et $Q = 2X^2 + Y^2 - Y - 2$. Calculer le résultant $\text{Res}_Y(P, Q)$.

- 5.d. Déterminer les points d'intersection des ellipses d'équations $P = 0$ et $Q = 0$.
6. Soit n un entier ≥ 1 . Posons $P = (X - 1)^n - (X^n - 1) \in \mathbf{C}[X]$.
- 6.a. Déterminer les racines de P' .
- 6.b. Pour quelles valeurs de n le polynôme P admet-il une racine multiple ?
7. On dit qu'un nombre complexe est un *entier algébrique* s'il existe $P \in \mathbf{Z}[X]$ unitaire tel que $P(x) = 0$.
- 7.a. Soient $P, Q \in \mathbf{Z}[X]$ unitaires. Montrer que $\text{Res}_X(P(X+Y), Q(X))$ est unitaire dans $\mathbf{Z}[Y]$.
- 7.b. Montrer que la somme de deux entiers algébriques est un entier algébrique.
- 7.c. Montrer que le produit de deux entiers algébriques est un entier algébrique.
- 7.d. L'anneau des entiers algébriques est-il intègre, principal, factoriel, noethérien, artinien ?
8. Exprimer les polynômes symétriques suivants en fonction des polynômes symétriques élémentaires : $X^3 + Y^3 + Z^3, X^2Y + XY^2 + X^2Z + XZ^2 + Y^2Z + YZ^2, X^2YZ + XY^2Z + XYZ^2, X^4 + Y^4 + Z^4$.
- 9.a. Soient $a, b, c \in \mathbf{C}$. Montrer qu'ils sont en progression arithmétique (resp. géométrique) si et seulement si $27abc = (a+b+c)(9(ab+bc+ac) - 2(a+b+c)^2)$ (resp. $(ab+ac+bc)^3 = abc(a+b+c)^3$).
- 9.b. Soient $\alpha, \beta, \gamma, \delta \in \mathbf{C}$ les racines de $X^4 + X + 1$. Calculer $1/(\alpha-1) + 1/(\beta-1) + 1/(\gamma-1) + 1/(\delta-1)$.
- 9.c. Soient α, β, γ les racines de $X^3 + 2X^2 - 2X + 5$. Trouver un polynôme de $\mathbf{Z}[X]$ de racines $\alpha^3, \beta^3, \gamma^3$.
- 9.d. Soit $P = X^3 + 2X^2 + 3X + 4 \in \mathbf{Q}[X]$. Notons α, β, γ ses racines complexes. Déterminer le polynôme unitaire de degré 3 dont les racines sont $\alpha + \beta, \beta + \gamma$ et $\alpha + \gamma$.
- 9.e. Soit $P = X^3 + X + 1 \in \mathbf{Q}[X]$. Notons α, β, γ ses racines complexes. Calculer $\alpha + \beta + \gamma, \alpha^2 + \beta^2 + \gamma^2, \alpha^3 + \beta^3 + \gamma^3$ et, en calculant la division euclidienne de X^4 par $P, \alpha^4 + \beta^4 + \gamma^4$.
10. Soit K un corps. Soit $P \in K[X]$ sans facteur multiple.
- 10.a. Soit $Q \in K[X]$ un polynôme sans facteur multiple premier à P . Montrer que le discriminant de PQ est un carré dans K si et seulement si le produit des discriminants de P et Q est un carré dans K . Rappelons qu'il se décompose en produits de facteurs irréductibles de degrés 1 ou 2 dans $\mathbf{R}[X]$.
- 10.b. Supposons $P \in \mathbf{R}[X]$. Rappelons qu'il se décompose en produits de facteurs irréductibles de degrés 1 ou 2 dans $\mathbf{R}[X]$. Soit $Q \in \mathbf{R}[X]$ un polynôme irréductible de degré 2 (resp. 1) premier à P . Montrer que le discriminant de PQ est de signe opposé (resp. égal) à celui du discriminant de P .
- 10.c. Supposons encore $P \in \mathbf{R}[X]$. En déduire que le discriminant de P est > 0 si et seulement si la décomposition de P dans $\mathbf{R}[X]$ comprend un nombre pair de facteurs de degré 2.
- 10.d. Soit p un nombre premier $\neq 2$. Supposons que $P \in \mathbf{F}_p[X]$. Montrer que si P est irréductible de degré impair (resp. pair) le discriminant de P est (resp. n'est pas) un carré dans \mathbf{F}_p .
- 10.e. Supposons que $P \in \mathbf{F}_p[X]$. Montrer que le discriminant de P est un carré si et seulement si la décomposition en produit de facteurs irréductibles de P comprend un nombre pair de facteurs de degré pair.
11. Soit $P \in \mathbf{R}[X]$ tel que pour tout $a, b, c \in \mathbf{R}$ tel que $ab+ac+bc = 0$ on ait $P(a-b) + P(b-c) + P(c-a) = 2P(a+b+c)$.
- 11.a. Trouver a, b, c non nuls dans \mathbf{Z} tels que $ab+ac+bc = 0$.
- 11.b. En considérant les triplets ax, bx, cx pour $x \in \mathbf{R}$, montrer que P est somme d'un monôme de degré 2 et d'un monôme de degré 4.
12. Trouver tous les polynômes $P \in \mathbf{R}[X]$ tels que pour tout réels a, b, c , on ait : $P(a+b-2c) + P(b+c-2a) + P(c+a-2b) = 3(P(a-b) + P(b-c) + P(c-a))$.
13. 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 .
- 13.a. 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.
- 13.b. 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} .
- 13.c. Montrer que les polynômes $R_j + R_{j^2}$ et $R_j R_{j^2}$ sont symétriques. Les exprimer en fonctions des polynômes symétriques élémentaires.
- 13.d. 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 .
- 13.e. Exprimer α, β et γ en fonction de u et v .

14. Soit K un corps de caractéristique différente de 2 et 3. Soit $P = X^4 + aX^2 + bX + c \in K[X]$. Supposons-le scindé de racines $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. On se propose de déterminer ces racines en fonctions de a, b et c .

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

14.b. Établir que le coefficient en X du polynôme $R(X) = (X - U)(X - V)(X - W) \in K[X_1, X_2, X_3, X_4][X]$ est symétriques en X_1, X_2, X_3, X_4 . Exprimer ce coefficient en terme des polynômes symétriques élémentaires.

14.c. Exprimer $\alpha_1, \alpha_2, \alpha_3$ 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 $W(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.

14.d. Conclure à l'aide de l'exercice précédent.

15. Soit n un entier > 0 . Notons E_n l'ensemble des polynômes de $\mathbf{Z}[X]$ unitaires de degré n et dont toutes les racines sont de module 1.

15.a. Soit ζ une racine de l'unité dans \mathbf{C} . Montrer que toutes les racines de son polynôme minimal sur \mathbf{Q} sont de module 1.

15.b. Montrer que E_n est fini.

15.c. Pour $P \in E_n$ de racines x_1, x_2, \dots, x_n , on note P_2 le polynôme unitaire de racines $x_1^2, x_2^2, \dots, x_n^2$. Montrer que $P_2 \in \mathbf{Z}[X]$.

15.d. En déduire que les racines de P sont des racines de l'unité.

15.e. À quelle condition sur le nombre réel x existe-t-il $P \in \mathbf{Z}[X]$ unitaire tel que $P(e^{2i\pi x}) = 0$.

16. Soit K un corps. Soient $P, Q \in K[X]$ deux polynômes non constants ayant les mêmes racines. Notons p_0 et p_1 le nombre de racines de P et $P - 1$ respectivement. Supposons que $P - 1$ et $Q - 1$ aient eux aussi les mêmes racines. Notons n le degré de P et supposons que le degré de Q est $\leq n$.

16.a. Montrer que le polynôme $P - Q$ admet au moins $p_0 + p_1$ racines.

16.b. Montrer que $D_0 = \text{pgcd}(P, P')$ et $D_1 = \text{pgcd}(P - 1, P')$ sont de degrés $n - p_0$ et $n - p_1$ respectivement.

16.c. Montrer que D_0D_1 divise P' . En déduire que $p_0 + p_1 > n$, puis que $P = Q$.

17. Soit n des entiers ≥ 1 . Soit K un corps. Considérons des n -uplets $(a_i)_{1 \leq i \leq n}$ et $(b_j)_{1 \leq j \leq n}$ des n -uplets dans K^n . On suppose que la quantité $\prod_i (b_j - a_i)$ ne dépend pas de j . Notons-la c .

17.a. Posons $A = \prod_i (X - a_i)$ et $B = \prod_j (X - b_j)$ dans $K[X]$. Montrer que $A - c = B$.

17.b. En déduire que la quantité $\prod_j (b_j - a_i)$ ne dépend pas de i .

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

18.a. Soient i et $j \in \{1, \dots, n\}$ deux entiers distincts. Notons $\phi_{i,j}$ l'homomorphisme d'anneaux $A \rightarrow A$ 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 $\phi_{i,j}$.

18.b. Montrer que $T_i - T_j$ divise V dans A ($1 \leq i, j \leq n, i \neq j$) puis que $V = \prod_{i < j} (T_j - T_i)$.

18.c. Soient i, i', j et $j' \in \{1, \dots, n\}$ tels que $\{i, j\} \neq \{i', j'\}$. 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 : $(V) = \cap_{i < j} (T_i - T_j)$.

18.d. Montrer P est alterné si et seulement si il existe un polynôme symétrique $Q \in A$ tel que $P = QV$.

18.e. 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 $P = QV + R$.

18.f. Cette dernière propriété est-elle encore vérifiée si la caractéristique de K est 2 ?

19. Soit r un entier > 0 . Une *partition de longueur r* est r -uplet décroissant d'entiers > 0 . Si $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r)$ est une telle partition, on dit que $|\lambda| = \lambda_1 + \lambda_2 + \dots + \lambda_r$ est le *poids* de λ . On note $\Pi(r)$ l'ensemble des r -uplets $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r)$ tels qu'il existe $s \leq r$ avec $(\lambda_1, \lambda_2, \dots, \lambda_s)$ partition de longueur s . On note $\Pi^+(r)$ les r -uplets de $\Pi(r)$ qui sont strictement décroissants.

Soit n un entier ≥ 1 . On rappelle que l'anneau factoriel $\mathbf{Z}[X_1, X_2, \dots, X_n]$ est muni de l'action du groupe symétrique \mathcal{S}_n . On note $\epsilon(\sigma)$ la signature d'une permutation $\sigma \in \mathcal{S}_n$. Un polynôme P en n indéterminées est dit *alterné* si on a $\sigma.P = \epsilon(\sigma)P$ pour tout $\sigma \in \mathcal{S}_n$. On note A_n l'ensemble des polynômes alternés.

19.a. Soit $P \in A_n$. Montrer que P est divisible par $X_i - X_j$ ($i, j, 1 \leq i < j \leq n$). Posons $A = \prod_{i < j} (X_i - X_j)$.

19.b. Montrer que A_n est un module sur l'anneau des polynômes symétriques engendré par A .

19.c. Soit $R \in \mathbf{Z}[X_1, X_2, \dots, X_n]$ un polynôme invariant sous l'action des permutations paires mais pas sous \mathcal{S}_n . Montrer que l'orbite de R sous \mathcal{S}_n comprend deux éléments, notés R et S .

- 19.d. Montrer que $R + S$ est symétrique et que $R - S$ est alterné.
- 19.e. Le polynôme R est-il de la forme $P + AQ$ avec P et Q symétriques ?
- 19.f. Soit $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r) \in \Pi(r)$. Posons $A_\lambda = |X_i^{\lambda_j}|_{1 \leq i \leq r, 1 \leq j \leq n} \in \mathbf{Z}[X_1, X_2, \dots, X_r]$. Montrer que $A_\lambda \in A_n$ est homogène de degré $|\lambda|$. Que se passe-t-il lorsque $\lambda \notin \Pi^+(r)$?
- 19.i. Posons $\rho = (r-1, r-2, \dots, 1, 0) \in \Pi(r)$. Factoriser A_ρ .
- 19.j. Pour k entier $0 \leq k \leq n$, posons $\rho_k = (r, r-1, \dots, k+1, k-1, \dots, 1, 0)$. Calculer A_{ρ_k} .
- 19.k. Montrer que $(A_\lambda)_{\lambda \in \Pi^+(r)}$ est une base du \mathbf{Z} -module A_n .
- 19.l. Pour $\lambda \in \Pi(r)$, montrer que A_λ/A_ρ est symétrique.
- 19.m. Montrer que l'application $\Pi(r) \rightarrow \Pi^+(r)$ qui à λ associe $\lambda + \rho$ est bijective.
- 19.n. Pour $\lambda \in \Pi(r)$, le polynôme $A_{\lambda+\rho}/A_\rho$ s'appelle la *fonction de Schur* de λ . Montrer que les fonctions de Schur constituent une base des polynômes symétrique de $\mathbf{Z}[X_1, X_2, \dots, X_r]$.
20. Soit K un corps commutatif. Soit n un entier > 0 . Considérons $L = K((A_{i,j})_{1 \leq i, j \leq n}, (B_{i,j})_{1 \leq i, j \leq n})$ (corps des fractions rationnelles en $2n^2$ indéterminées).
- 20.a. Considérons les matrices $A = (A_{i,j})_{1 \leq i, u \leq n}$, $B = (B_{i,j})_{1 \leq i, u \leq n} \in M_n(L)$. Donner leurs déterminants et montrer que ces derniers sont non nuls. Les matrices A et B sont-elles inversibles dans $M_n(L)$?
- 20.b. Soient $M, N \in M_n(L)$ inversibles. Montrer que les matrices $XI_n - MN$, $XI_n - NM \in M_n[L(X)]$ sont conjuguées. En déduire que les polynômes caractéristiques de MN et de NM sont égaux.
- 20.c. 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 .
- 20.d. Soit $A_0 = (\alpha_{i,j})_{1 \leq i, j \leq n}$ et $B_0 = (\beta_{i,j})_{1 \leq i, j \leq n} \in M_n(K)$. 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.
21. Soit K un corps de caractéristique 0. Soit n un entier ≥ 0 . Soient $A, B \in M_n(K)$,
- 21.a. Soient $P, Q \in K[X]$ unitaires, de degré n , scindés de racines $\lambda_1, \lambda_2, \dots, \lambda_n$ et $\mu_1, \mu_2, \dots, \mu_n$ respectivement. Montrer que si, pour tout entier i , $0 \leq i \leq n$, on a $\sum_{j=1}^n \lambda_j^i = \sum_{j=1}^n \mu_j^i$, on a $P = Q$.
- 21.b. Supposons que pour tout $i \in \{1, 2, \dots, n\}$, A^i et B^i aient même trace. Montrer que A et B ont même polynôme caractéristique.
- 21.c. Supposons A^i de trace nulle ($i \in \{1, 2, \dots, n\}$). Montrer que A est nilpotente.
- 21.d. Supposons A^i de trace nulle ($i \in \{1, 2, \dots, n-1\}$). Montrer que A est nilpotente ou diagonalisable.
22. Soit K un corps. Soit n un entier ≥ 1 . Soit $F \in K(X_1, X_2, \dots, X_n)$ une fraction rationnelle symétrique.
- 22.a. Montrer que F peut s'écrire comme une fraction rationnelle en $\Sigma_1, \Sigma_2, \dots, \Sigma_n$.
- 22.b. Montrer que les fractions rationnelles symétriques constituent un sous-corps L de $K(X_1, X_2, \dots, X_n)$ isomorphe à $K(X_1, X_2, \dots, X_n)$.
- 22.c. Les éléments X_1, X_2, \dots, X_n sont-ils algébriques sur L . Donner les polynômes minimaux.
- 22.d. L'extension $K(X_1, X_2, \dots, X_n)|L$ est-elle algébrique ? Finie ?
23. Soit n un entier ≥ 1 . Soit K un corps algébriquement clos. Soient $F_1, F_2, \dots, F_m \in K[X_1, X_2, \dots, X_n]$ sans zéro commun. On va montrer Z_n par récurrence sur n : il existe $H_1, H_2, \dots, H_m \in K[X_1, X_2, \dots, X_n]$ tels que $1 = F_1H_1 + F_2H_2 + \dots + F_mH_m$ (Version faible du *théorème des zéros*, ou encore *Nullstellensatz*, de Hilbert).
- 23.a. Montrer Z_1 .
- 23.b. Soit $P \in K[X_1, X_2, \dots, X_n]$ non nul de degré d . Montrer qu'il existe $(a_1, a_2, \dots, a_{n-1}) \in K^{n-1}$, $c \in K$ et $Q \in K[X_1, X_2, \dots, X_n]$ de degré $< d$ en X_n tel que $P(X_1 + a_1X_n, \dots, X_{n-1} + a_{n-1}X_n, X_n) = cX_n^d + Q$.
- 23.c. Montrer qu'on peut se ramener au cas où F_1 est unitaire pour montrer Z_n en supposant Z_{n-1} .
- 23.d. Posons $G(Y, X_1, X_2, \dots, X_n) = F_2 + YF_3 + \dots + Y^m F_{m-2} \in K[Y, X_1, X_2, \dots, X_n]$. Montrer qu'il existe $A, B \in K[Y, X_1, X_2, \dots, X_n]$ tels que $\text{Res}_{X_n}(F_1, G) = AG + BF_1$.
- 23.e. Posons $\text{Res}_{X_n}(F_1, G) = P_k(X_1, X_2, \dots, X_{n-1})Y^k + \dots + P_0(X_1, X_2, \dots, X_{n-1})$. Montrer que P_0, P_1, \dots, P_k n'ont pas de zéro commun, et engendre donc un sous-module contenant 1, par hypothèse de récurrence.
- 23.f. Montrer que les polynômes P_0, P_1, \dots, P_k sont dans l'idéal engendré par F_1, F_2, \dots, F_m . En déduire Z_n .
- 23.g. Soit I un idéal de $K[X_1, X_2, \dots, X_n]$. Posons $V(I) = \{(x_1, \dots, x_n) \in K^n / f(x_1, \dots, x_n) = 0 (f \in I)\}$. Soit $g \in K[X_1, X_2, \dots, X_n]$ s'annule sur $V(I)$. Introduisons l'indéterminée supplémentaire X_0 . Montrer que les polynômes $F_1, F_2, \dots, F_m, 1 - X_0g \in K[X_0, X_1, X_2, \dots, X_n]$ sont sans zéro commun. En déduire que si $g \in K[X_1, X_2, \dots, X_n]$ s'annule sur $V(I)$, il existe un entier $k > 0$ tel que $g^k \in I$ (véritable théorème des zéros).