Feuille n^o 4
jeudi 23 janvier
Polynômes à plusieurs variables

Exercice 1 Polynômes homogènes.

Soit K un corps. Montrer que $\dim_K K[X_0, ..., X_n]_d = \binom{n+d}{d}$.
Indication : considérer la série $\frac{1}{(1-X)^d}$.

Exercice 2 Polynômes symétriques

Si $s \in \mathfrak{S}_n$, si $P \in \mathbb{Z}[X_1, ..., X_n]$, on note $P^s(X_1, ..., X_n) := P(X_{s(1)}, ..., X_{s(n)})$. (*C'est une action à droite*). On note $\mathbb{Z}[X_1, ..., X_n]^{\mathfrak{S}_n}$ les polynômes invariants ou *polynômes symétriques.*

On note $\sigma_{k,n}(X_1, ..., X_n) := \sum_{1 \leq i_1 < ... < i_k \leq n} X_{i_1} ... X_{i_k}$ les *polynômes symétriques élémentaires.*

On peut aussi les définir par l'égalité :

$$(T + X_1)....(T + X_n) = T^n + \sigma_{1,n}T^{n-1} + ... + \sigma_{n,n}$$

dans $\mathbb{Z}[X_1, ..., X_n][T]$.

a) En raisonnant par récurrence sur le degré donné par l'ordre lexicographique $X_1 > ... > X_n$, montrer que $\mathbb{Z}[X_1, ..., X_n]^{\mathfrak{S}_n} = \mathbb{Z}[\sigma_1, ..., \sigma_n]$. *Indication : montrer que si* $a_1 \geq ... \geq a_n$*, alors les polynômes* $X_1^{a_1} ... X_n^{a_n}$ *et* $\sigma_{1,n}^{a_1 - a_2} ... \sigma_{n,n}^{a_n - a_{n-1}}$ *ont le même terme dominant.*

b) On note $\mathfrak{A}_n$ le groupe des permutations paires. Montrer que $\mathbb{Z}[X_1, ..., X_n]^{\mathfrak{A}_n} = \mathbb{Z}[\sigma_1, ..., \sigma_n] + \Delta\mathbb{Z}[\sigma_1, ..., \sigma_n]$ où $\Delta := \prod_{1 \leq i < j \leq n}(X_i - X_j)$.
Indication : soit P *tel que* $^\forall \sigma$, $P^\sigma = \epsilon(\sigma)P$*, alors* P *est divisible par* Δ *(raisonner par récurrence)*

Exercice 3 $\mathbb{C}$ est algébriquement clos

d'après P. Samuel, Théorie algébrique des nombres, appendice du chap. II

a) Soit $P \in \mathbb{R}[X]$ de degré impair. Montrer que P a une racine réelle. *Indication : utiliser le TVI !*

b) Soit $P \in \mathbb{R}[X]$ de degré n. On factorise dans une extension de $\mathbb{C}$. On note $x_1, ..., x_n$ les racines (éventuellement avec des répétitions).
On raisonne par récurrence sur $v_2(n)$, l'exposant de la plus grande puissance de 2 qui divise n. Montrer que P a une racine complexe. *Indication : si* $c \in \mathbb{R}$*, considérer le polynôme* $\prod_{1 \leq i < j \leq n} X - (x_i + x_j + cx_ix_j)$ *est à coefficients réels et en déduire qu'il a au moins une racine complexe ; puis utiliser que* $\mathbb{R}$ *est infini pour trouver deux réels* $c \neq c'$ *et* $1 \leq i < j \leq n$ *tels que*

$$x_i + x_j + cx_ix_j \text{ et } x_i + x_j + c'x_ix_j \in \mathbb{C}$$

...

Exercice 4 Discriminant

Soit $P = a_0X^n + ... + a_n \in \mathbb{C}[X]$ un polynôme de degré $n \geq 1$.

On suppose que $P = a_0(X - x_1)...(X - x_n)$.

On pose $\Delta_P = a_0^{2n-2} \prod_{1\leq i<j\leq n}(x_i - x_j)^2 = a_0^{2n-2}(-1)^{\frac{n(n-1)}{2}} \prod_{1\leq i\neq j\leq n}(x_i - x_j)$.

a) Montrer que $\Delta_P \in \mathbb{Z}[a_0, ..., a_n]$.

b) Calculer Δ_P si P est de degré 2.

c) Si P est de degré 3, montrer que

$$\Delta_P = a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 - 27a_0^2a_3^2 + 18a_0a_1a_2a_3 \ .$$

Indications : Montrer que $\Delta = a\sigma_1^6 + b\sigma_1^4\sigma^2 + c\sigma_1^3\sigma_3 + d\sigma_1^2 + e\sigma_1\sigma_2\sigma_3 + f\sigma_2^3 + g\sigma_3^2$; puis en prenant $x_3 = 0$, montrer que $a = b = 0$ et trouver d, f. Puis traiter le cas où $\sigma_2 = 0$, etc

d) Montrer que $\Delta_P = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n P'(x_i)$ si P est unitaire.

e) Montrer que P est à racines simples $\Leftrightarrow \Delta_P \neq 0 \Leftrightarrow P' \wedge P = 1$.

f) Calculer le discriminant de $X^n - 1$.

Exercice 5 Soit K un corps. On note $K[[X]]$ l'anneau des séries formelles à coefficients dans K avec :

$$\sum_{n\geq 0} a_nX^n + \sum_{n\geq 0} b_nX^n = \sum_{n\geq 0}(a_n + b_n)X^n$$

$$(\sum_{n\geq 0} a_nX^n)(\sum_{n\geq 0} b_nX^n) = \sum_n(\sum_{k=0}^n a_kb_{n-k})X^n \ .$$

a) Soit $(S_k)_{k\in\mathbb{N}}$ une suite de séries formelles.

On suppose que

$$^\forall n,\ S_k[n] = 0 \text{ si } k >> 0$$

(où $S_k[n]$ est le coefficient devant X^n de la série S_k).

On pose :

$$\sum_{k\geq 0} S_k := \sum_{n\geq 0}(\sum_{k\geq 0} S_k[n])X^n \ .$$

Par exemple si $X|S$, $\sum_{k\geq 0} S^k = \frac{1}{1-S}$.

Vérifier que

$$\sum_{k\geq 0} S_k^1 + \sum_{k\geq 0} S_k^2 = \sum_{k\geq 0}(S_k^1 + S_k^2)$$

$$S(\sum_{k\geq 0} S_k) = \sum_{k\geq 0} SS_k,$$

$$\sum_{k\geq 0} S_k' = (\sum_{k\geq 0} S_k)' \ .$$

b) On suppose K de caractéristique nulle. Si $S \in k[[X]]$ et si $S_0 = 1$, on pose :

$$\log S = \sum_{k \geq 1} \frac{(-1)^{k-1}}{k} (S-1)^k \quad .$$

Vérifier que $(\log S)' = \frac{S'}{S}$. En déduire que si $S_{1,0} = S_{2,0} = 1$, alors

$$\log(S_1 S_2) = \log S_1 + \log S_2 \quad .$$

Exercice 6 Sommes de Newton. Soient $c_1, ..., c_n \in \mathbb{Z}[X_1, ..., X_n]$ les polynômes symétriques tels que :

$$\prod_{i=1}^{n} (1 - X_i T) = 1 + \sum_{i=1}^{n} c_i T^i$$

dans l'anneau $\mathbb{Z}[X_1, ..., X_n][T]$. On pose pour tout k : $S_k = X_1^k + ... + X_n^k$.

a) Exprimer $X_1^3 + X_2^3 + X_3^3$ à l'aide des c_i. *Indication : remplacer dans l'identité ci-dessus T par $\frac{1}{X_i}$, $i = 1, 2, 3$.*

b) Montrer que :

$$S_r + c_1 S_{r-1} + ... + c_{r-1} S_1 + c_r r = 0$$

pour tout $r \geq 0$ (où on convient que $c_k = 0$ si $k < 0$ et $c_0 = 1$).

Indication : commencer par le cas où $r = n$ puis $r \geq n$. Pour le cas où $r < n$, considérer le polynôme $F = S_r + c_1 S_{r-1} + ... + c_{r-1} S_1 + c_r r$ puis $F(X_1, ..., X_r, 0, ..., 0)$ ...

Ce sont les formules de Girard-Newton

c) **Formules de Waring.**

On pose $C(T) = \sum_{i=1}^{n} c_i T^i$. En calculant $\log(1 + C)$, montrer que

$$\frac{\sum_{r \geq 1} S_r T^r}{r} = \sum_{k \geq 1} \frac{(-1)^k}{k} C^k \quad .$$

d) En déduire que :

$$\frac{S_r}{r} = \sum_{\substack{k_1, ..., k_n \geq 0 \\ k_1 + 2k_2 + ... + nk_n = r}} (-1)^{k_1 + ... + k_n} \frac{(k_1 + ... + k_n - 1)!}{k_1! ... k_n!} c_1^{k_1} ... c_n^{k_n} \quad .$$

pour tout $r \geq 1$.

Exercice 7 Résultant. Soient $P := a_0X^p + ... + a_p, Q := b_0X^q + ... + b_q \in A[X]$ où A est un anneau.

Soit $\text{Rés}_{p,q}(P,Q)$ le déterminant de la matrice :

$$\begin{array}{r} q \text{ lignes} \\ \\ p \text{ lignes} \end{array} \begin{pmatrix} a_0 & a_1 & \dots & a_p & & & \\ & a_0 & a_1 & \dots & a_p & & \\ & & \ddots & \ddots & & \ddots & \\ b_0 & b_1 & \dots & b_q & & & \\ & b_0 & b_1 & \dots & b_q & & \\ & & \ddots & \ddots & & \ddots & \end{pmatrix}$$

Le coefficient (i,j) de la matrice est : a_{j-i} si $1 \leq i \leq q$ et b_{j-i+q} si $q+1 \leq i \leq p+q$ *(où l'on convient que $a_n = 0$ si $n < 0$).*

a) Soit K un corps. Montrer que si $P, Q \in K[X]$ sont de degrés respectifs p, q, alors $\text{Rés}_{p,q}(P,Q) = 0 \Leftrightarrow P, Q$ ont un facteur commun.
Indication : vérifier d'abord que P, Q ont un facteur commun si et seulement si $PF = QG$ pour certains polynômes F, G non nuls de degrés $< q$ et $< p$ respectivement. Puis trouver dans de bonnes bases la matrice de l'application linéaire :

$$K[X]_{<q} \oplus K[X]_{<p} \to K[X]_{<p+q}\,,\ F \oplus G \mapsto PF + QG\ .$$

b) Montrer que si $P = a_0(X-x_1)...(X-x_p)$ et $Q = b_0(X-y_1)...(X-y_q)$, alors

$$\text{Rés}(P,Q) = a_0^q b_0^p \prod_{i=1,j=1}^{i=p,j=q} (x_i - y_j)\ .$$

Indication : on pourra raisonner dans l'anneau des polynômes $\mathbb{Z}[a_0, b_0, x_1, ..., x_p, y_1, ...y_q]$ en $pq+2$ variables : les deux polynômes ont les mêmes degrés en les y_j et on peut comparer les termes dominants pour l'ordre lexicographique $y_1 > ... > y_q$ par exemple.

c) En déduire que $a_0^q \prod_{i=1}^p Q(x_i) = (-1)^{pq} b_0^p \prod_{j=1}^q P(y_j)$.

d) En déduire aussi : $\text{Rés}_{p,q}(P,Q) = (-1)^{pq}\text{Rés}_{q,p}(Q,P)$.

Exercice 8 Démonstration de la loi de réciprocité quadratique au moyen du résultant.

a) Vérifier que pour tout $k \geq 1$, il existe un polynôme $P \in \mathbb{Z}[X]$ tel que $X^k + \frac{1}{X^k} = P\left(X + \frac{1}{X}\right)$.
Soit p un nombre premier impair.
On note $T_p \in \mathbb{Z}[X]$ unitaire de degré $\frac{p-1}{2}$ tel que :

$$X^{(p-1)/2} T_p\left(X + \frac{1}{X}\right) = 1 + ... + X^{p-1}\ .$$

b) Montrer que $T_p(0) = \pm 1$.

c) Montrer que si $p \neq q$ sont premiers impairs, alors : $\text{Rés}(T_p, T_q) = \pm 1$.
Indication : si r est un nombre premier qui divise $\text{Rés}(T_p, T_q)$, alors les polynômes T_p et T_q quraient une racine commune dans une extension du corps $\mathbb{F}_r$ ...

d) $\text{Rés}(T_p, T_q) = \left(\frac{q}{p}\right) \bmod p$. *Indication : Réduire $\bmod p$, que vaut T_p dans $\mathbb{F}_p[X]$?*

e) En déduire la loi de réciprocité quadratique :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \quad .$$