Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

TD 5

Exercice 1.
Evaluer la complexité du critère d'irréductibilité d'un polynôme sans facteur multiple $F \in \mathbb{F}_p[X]$, puis celle de l'algorithme de Berlekamp.

Exercice 2.
Soient $f \in \mathbb{Z}[X]$ et $n = \deg(f)$, montrer que l'on a

$$|\mathrm{discrim}_X(f)| \leq n^n (n+1)^{2n-2} ||f||_\infty^{2n-2}$$

(*indication :* on pourra montrer que $|\mathrm{discrim}_X(f)| \leq n^n M(f)^{2n-2}$ en appliquant le lemme de Hadamard au déterminant de Van der Monde)

Exercice 3.

1. Soit K un corps commutatif ; on désignera par $K[X]_{\leq n}$ l'espace vectoriel formé du polynôme nul et des polynômes de degré $\leq n$.
   Soit $x = (x_1, \cdots, x_{n+1})$ une suite de $n+1$ éléments de K *deux à deux distincts* ; alors montrer que l'application linéaire :

$$\begin{array}{rcl} L_x : K[X]_{\leq n} & \longrightarrow & K^{n+1} \\ f & \longrightarrow & (f(x_1), \cdots, f(x_{n+1})) \end{array}$$

   est bijective.
   Pour $1 \leq i \leq n+1$, considérons le polynôme :

$$L_{x,i} = \frac{\prod_{k \neq i} (X - x_k)}{\prod_{k \neq i} (x_i - x_k)}$$

   Pour tout $y = (y_1, \cdots, y_{n+1}) \in K^{n+1}$, on pose $f = \sum_{i=1}^{n+1} y_i L_{x,i} \in K[X]_{\leq n}$; montrer que $L_x(f) = y$ (polynômes d'interpolation de Lagrange).
2. Soit $f \in \mathbb{Z}[X]$ un polynôme primitif de degré n avec $n = 2s$ ou $n = 2s+1$.
   On fixe une suite strictement croissante d'entiers $(x_1, \cdots, x_{s+1})$ dont aucune n'est racine de f.
   Soit $g \in \mathbb{Z}[X]$ un diviseur de f de degré $\leq s$; montrer que g est déterminé de manière unique par les entiers $y_i = g(x_i)$ pour $1 \leq i \leq s+1$ et que l'on a $y_i | f(x_i)$ pour $1 \leq i \leq s+1$.
   En déduire un algorithme permettant de factoriser f (*algorithme de Kronecker*).