TD 5 : Résultant de polynômes

Théorème fondamental de l'algèbre.
Tout corps K possède une *clôture algébrique* $\bar{\mathsf{K}}$, telle que $\mathsf{K} \subset \bar{\mathsf{K}}$ et tout polynôme F de degré m à coefficients dans K possède exactement m racines dans $\bar{\mathsf{K}}$ (en comptant avec multiplicité). Si l'on note f_m le coefficient dominant de F et $\alpha_1, \dots, \alpha_m$ ses racines, alors $F(X) = f_m \prod_{i=1}^m (X - \alpha_i)$.

Exercice.
Soit F et G deux polynômes de degrés m et n, respectivement, à coefficients dans un corps K. On note $x_1, \dots, x_m$ les racines de F et $y_1, \dots, y_n$ celles de G, dans $\bar{\mathsf{K}}$. Le *résultant* de F et G est défini [1] par

$$\operatorname{res}(F, G) = f_m^n g_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (x_i - y_j)$$

où f_m est le coefficient dominant de F et g_n celui de G, avec la convention que $\operatorname{res}(F, 0) = 0$.

1. **Propriétés.**
   - **i.** Donner la valeur de $\operatorname{res}(F, \lambda)$ où λ est une constante.
   - **ii.** Montrer que $\operatorname{res}(F, G) = (-1)^{mn} \operatorname{res}(G, F)$.
   - **iii.** Montrer que $\operatorname{res}(F, G) = (-1)^{mn} g_n^m \prod_{j=1}^n F(y_j) = f_m^n \prod_{i=1}^m G(x_i)$.
   - **iv.** Soit $F = QG + R$ la division euclidienne de F par G ($\deg(R) < \deg(G)$). Montrer que $\operatorname{res}(F, G) = (-1)^{mn} g_n^{m-r} \operatorname{res}(G, R)$ où $r = \deg(R)$.
2. **Algorithmes.**
   - **i.** Déduire des questions précédentes un algorithme de type Euclide pour calculer le résultant de deux polynômes.
   - **ii.** En généralisant l'algorithme précédent à un algorithme de type « Euclide étendu », montrer que pour tout F et G, il existe deux polynômes U et V tels que $\operatorname{res}(F, G) = FU + GV$.
   - **iii.** Déduire des algorithmes précédents que $\operatorname{res}(F, G) \in \mathsf{K}$.
   - **iv.** *(Bonus)* Adapter l'algorithme du demi-PGCD au résultant.
3. **Lien avec le pgcd.** Montrer que $\operatorname{res}(F, G) = 0$ si et seulement si $\deg(\operatorname{pgcd}(F, G)) > 0$.
4. **Discriminant.** On définit le *discriminant* d'un polynôme F de degré m par

   $$\operatorname{disc}(F) = (-1)^{m(m-1)/2} \frac{1}{f_m} \operatorname{res}(F, F')$$

   où F' est la dérivée de F et f_m son coefficient dominant.
   - **i.** Calculer le discriminant de $F = aX^2 + bX + c$.
   - **ii.** Montrer que $\operatorname{disc}(F) = f_m^{2(m-1)} \prod_{1 \leq i < j \leq m} (\alpha_i - \alpha_j)^2$ où $\alpha_1, \dots, \alpha_m$ sont les racines de F dans $\bar{\mathsf{K}}$.
   - **iii.** En déduire que si F est un polynôme à coefficients réels ayant m racines réelles, $\operatorname{disc}(F) > 0$.

   Remarque. La réciproque n'est pas vraie. On sait simplement que si F est à coefficient réel et que $\operatorname{disc}(F) > 0$*, alors son nombre de racines réelles est congru à m modulo* 4*, et si* $\operatorname{disc}(F) < 0$*, alors son nombre de racines réelles est congru à* $m - 2$ *modulo* 4*. On retrouve le résultat habituel pour le degré* 2*.*

   - **iv.** *(Bonus)* Démontrer la remarque précédente.

1. On définit habituellement le résultant comme déterminant de la matrice de Sylvester associée à F et G (pour ceux qui connaissent !). La définition donnée ici est strictement équivalente.