MMA 数学特論I。多項式系のアルゴリズム: グレブナー基底 & 消去法
担当：DAHAN Xavier July 1st, 2010
TRA: 横山 Shun'ichi NAME：CORRECTION.

# Practice test IV: Resultant

- You can use any theorem, proposition or corollary of the class lectures, just by citing its number inside the corresponding lecture: (example: "Lect II, Cor. 1" refers to the Corollary 1 of Lecture II, that is the Primitive Element Theorem).

**Exercise 1** Write the Sylvester matrix of the polynomials $A$ and $B$:

| | | | |
|---|---|---|---|
| $A$ | $2x^2+x-1$ | $x-1$ | $x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ |
| $B$ | $30x^3+6x^2+x+1$ | $x+1$ | $3$ |

Answer:

$$\begin{pmatrix} 2 & 1 & -1 & 0 & 0 \\ 0 & 2 & 1 & -1 & 0 \\ 0 & 0 & 2 & 1 & -1 \\ 30 & 6 & 1 & 1 & 0 \\ 0 & 30 & 6 & 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 3 & & 0 \\ & 3 & \\ 0 & & \ddots \\ & & & 3 \end{pmatrix} \Big\} n \text{ times}$$

**Exercise 2** Are the following matrices in row echelon form ? *(the empty entries mean zero)*

$$A_1 = \begin{pmatrix} 4 & 1 & -1 & 1 & 0 \\ & & 4 & 1 & 1 \\ & & 1 & 0 & 0 \\ & & & & \end{pmatrix} \qquad A_2 = \begin{pmatrix} 1 & 1 & -1 & 3 & 1 & 0 \\ & & 2 & 3 & -2 & -3 \\ & & & -1 & -2 & 3 \\ & & & & & 2 \\ & & & & & \end{pmatrix}$$

$A_1$: No! $\qquad$ $A_2$: Ok!

**Exercise 3** Consider the 2 polynomials $A$ and $B$,

$$A = 2x^2 + x - 1 \qquad B = 30x^3 + 6x^2 + x + 1.$$

We have $\mathsf{Res}(A, B) = -1296$ *(sorry, I wrote 812, it was a mistake...)*

Given $n \in \mathbb{N}^*$, we consider the map $\phi_n : \mathbb{Z}[X] \to \mathbb{Z}/n\mathbb{Z}[X]$, $\sum_i a_i X^i \mapsto \sum_i (a_i \bmod n) X^i$.

Question 1 Use Proposition 1 to compute:

$$r_5 = \mathsf{Res}(\phi_5(A), \phi_5(B)) = \mathsf{Res}(A \bmod 5, B \bmod 5)$$

Answer: $\phi_5(\text{Res}(A,B)) = \phi_5(LC(A))^{\deg B - \deg \phi_5(B)} r_5$

$\phi_5(B) = (30 \bmod 5)x^3 + (6 \bmod 5)x^2 + x + 1$

$LC(A) = 2$.

$\Rightarrow \phi_5(\text{Res}(A,B)) = -1296 \bmod 5 = (2 \bmod 5)^{3-2} r_5 \Rightarrow 4 = 2 r_5 \Rightarrow \boxed{r_5 = 2}$

Same question for $r_3 = \text{Res}(\phi_3(A), \phi_3(B)) = \text{Res}(A \bmod 3, B \bmod 3)$

Answer: $\phi_3(\text{Res}(A,B)) = \phi_3(LC(A))^{\deg B - \deg \phi_3(B)} r_3$

$\phi_3(B) = x + 1$ $\quad \phi_3(\text{Res}(A,B)) = -1296 \bmod 3 = 0$.

$= (2 \bmod 3)^{3-1} = r_3 \bmod 3$

$\Rightarrow \boxed{r_3 = 0}$

Question 2 Can we use Proposition 1 (*sorry, I wrote Proposition 2*) to compute $r_2 = \text{Res}(\phi_2(A), \phi_2(B)) = \text{Res}(A \bmod 2, B \bmod 2)$ ? Compute anyway $r_2$.

Answer: To use Proposition 1, we need $\phi(LC(A)) \neq 0$ or $\phi(LC(B)) \neq 0$.

But $\phi_2(LC(A)) = \phi_2(LC(B)) = 0$, so we cannot use Prop. 1.

$\cdot\ \phi_2(A) = x - 1 \qquad \phi_2(B) = x + 1 \quad \Rightarrow r_2 = \begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix} = 2 \bmod 2 = 0.$

**Exercise 4** Let $R$ be an integral domain (Lect. II, Def. 7… like $R = \mathbb{Z}$ or $R = k[Y]$) Let $A, B, C \in R[X]$. Show the formula:

$$\text{Res}(AB, C) = \text{Res}(A, C)\text{Res}(B, C).$$

(*advice:* *use the formulas of Theorem 1, Slide 9*)

Answer: Let $K = \text{Frac}(R)$ (i.e. $K = \mathbb{Q}$ if $R = \mathbb{Z}$, $K = k(Y)$ if $R = k[Y]$)

Let $\overline{K}$ the algebraic closure of $K$.

All the roots of $A$, $B$ and $C$ are in $\overline{K}$. So we can write,

$A = a(X-\alpha_1)\cdots(X-\alpha_n) \qquad B = b(X-\beta_1)\cdots(X-\beta_m) \quad C = c(X-\gamma_1)\cdots(X-\gamma_r)$

By Eq. (1) of Theorem 1, we have:

$$\text{Res}(AB, c) = (ab)^r c^{m+n} \prod_{\substack{1\le i\le n\\ 1\le j\le r}} (\alpha_i - \gamma_j) \prod_{\substack{1\le i\le m\\ 1\le j\le r}} (\beta_i - \gamma_j)$$

$$= \left(a^r c^n \prod_{\substack{1\le i\le n\\ 1\le j\le r}} \alpha_i - \gamma_j\right)\left(b^r c^m \prod_{\substack{1\le i\le m\\ 1\le j\le r}} \beta_i - \gamma_j\right) = \text{Res}(A,C)\text{Res}(B,C)$$

**Exercise 5** Cf. File "`Test5-Ex6-correction.nb`" on the webpage !!!