Notes for MA591U, Spring 2001
(Symbolic Computation)

Resultants

QUESTION: Let $f, g \in k[x]$. When do f and g have a common factor?

SOLUTION: f and g have a common factor if and only if there exist $f_1, g_1 \in k[x]$ with $\deg f_1 < \deg f$, $\deg g_1 < \deg g$ such that

$$f_1 g - g_1 g = 0.$$

PROOF:

($\Rightarrow$) Suppose f and g have a common factor h. Define f_1 and g_1 by $f = f_1 h$ and $g = g_1 h$. Then

$$0 = f_1 g_1 h - f_1 g_1 h = f_1 g - g_1 f.$$

($\Leftarrow$) Assume that we know that $f_1 g + g_1 f = 0$. Then $f_1 g = -g_1 f$. Since $\deg g_1 < \deg g$ and *all* factors of g must divide $g_1 f$, *some* factor of g must divide f. Hence g and f have a common factor. (We have implicity used unique factorization.)

RESTATEMENT OF THE ABOVE: Let $\deg f = n$, $\deg g = m$. Then f, g have a common root iff $\exists \alpha_0, \ldots, \alpha_{n-1} \in k$ and $\exists \beta_0, \ldots, \beta_{m-1} \in k$ so that

$$0 = \left(\sum_{i=0}^{n-1} \alpha_i x^i \right) \left(\sum_{j=0}^{m} b_j x^j \right) + \left(\sum_{i=0}^{n} a_i x^i \right) \left(\sum_{j=0}^{m-1} \beta_j x^j \right).$$

Multiply this out and we have an expression

$$0 = (\alpha_0 b_0 + a_0 \beta_0) + (\alpha_1 b_0 + \alpha_0 b_1 + a_1 \beta_0 + a_0 \beta_1) x + \cdots$$

where all the coefficients must be zero. This fact defines a system of linear equations on the α_i and the β_j; we can write the system in matrix form as:

$$\begin{pmatrix}
b_0 & & & & a_0 & & & \\
b_1 & b_0 & & & a_1 & a_0 & & \\
 & b_1 & \ddots & & \vdots & a_1 & \ddots & \\
\vdots & & & b_0 & & \vdots & & \\
 & \vdots & & b_1 & a_n & & & a_0 \\
b_m & & & & & a_n & & \vdots \\
 & b_m & & \vdots & & & \ddots & \\
 & & \ddots & & & & & \\
 & & & b_m & & & & a_n
\end{pmatrix}
\begin{pmatrix}
\alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \\ \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{m-1}
\end{pmatrix} = 0.$$

Denote the leftmost matrix as R and we see that f and g have a common solution if and only if $\det R = 0$.

DEFINITION. The resultant $\text{Res}(f,g)$ is $\det R$, as defined above. We usually denote it

$$\text{Res}(f,g) = \begin{vmatrix} a_n & & \cdots & a_1 & a_0 & & & & \\ & a_n & & \cdots & a_1 & a_0 & & & \\ & & \ddots & & & & \ddots & & \\ & & & & a_n & & \cdots & a_1 & a_0 \\ b_m & & \cdots & & b_1 & b_0 & & & \\ & b_m & & \cdots & & b_1 & b_0 & & \\ & & \ddots & & & & & \ddots & \\ & & & b_m & & \cdots & & b_1 & b_0 \end{vmatrix}.$$

One can think of the Euclidean algorithm as putting this matrix in row-reduced form.

FACTS: *(See S. Lang,* Algebra*)* Let $f, g \in R[x]$ (a domain).

(1) Suppose $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ and $g(x) = b(x-\beta_1)\cdots(x-\beta_m)$. Then

$$\text{Res}(f,g) = a^m b^n \prod_{i,j}(\alpha_i - \beta_j).$$

(2) Note that f, g have a common root iff $\text{Res}(f,g) = 0$.

(3) Note also that $\text{Res}(f,g) = a^m \prod g(\alpha_i) = (-1)^{mn} b^n \prod f(\beta_i)$.

EXAMPLE: For which values of y do $f(x) = x^3 + x$ and $g(x) = 3yx^2 + y - 1$ have a common root in $\mathbb{C}$?

Use the fact that

$$\text{Res}(f,g) = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 3y & 0 & y-1 & 0 & 0 \\ 0 & 3y & 0 & y-1 & 0 \\ 0 & 0 & 3y & 0 & y-1 \end{vmatrix} = (y-1)(2y+1)^2.$$

Setting this latter expression to zero, we obtain the values $y = 1$ and $y = -1/2$, which correspond to the solutions $\{0, 1\}$ and $\{\pm i, -1/2\}$, respectively.