16 Algebra

16.9 Resultants and Resolvents (8 units)

Background material is contained in the Part IB course Groups, Rings and Modules. The later questions relate to material in the Part II course Galois Theory.

1 Introduction

The resultant of polynomials $f, g \in \mathbb{C}[x]$ is a polynomial in the coefficients of f and g that vanishes if and only if they have a common root. This project looks at some ways of computing the resultant and gives some applications. The final section is concerned with the Galois group of a polynomial, and for this we also need resolvents.

2 Resultants

The *resultant* of polynomials $f(x) = a\prod_{i=1}^{m}(x-\alpha_i)$ and $g(x) = b\prod_{i=1}^{n}(x-\beta_i)$ is

$$\mathrm{Res}(f,g) = a^n b^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j) = a^n \prod_{i=1}^{m} g(\alpha_i).$$

Question 1 Write a procedure for computing the resultant of two polynomials in $\mathbb{C}[x]$. (You may use any inbuilt procedure to compute the roots.) Test it on some polynomials with small integer coefficients and comment on the results.

The Sylvester matrix of $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_0$ is the $(m+n)\times(m+n)$ matrix

$$\begin{pmatrix}
a_m & a_{m-1} & \ldots & a_1 & a_0 & 0 & \ldots & 0 \\
0 & a_m & a_{m-1} & \ldots & a_1 & a_0 & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & \ldots & 0 & a_m & a_{m-1} & \ldots & a_1 & a_0 \\
b_n & b_{n-1} & \ldots & b_1 & b_0 & 0 & \ldots & 0 \\
0 & b_n & b_{n-1} & \ldots & b_1 & b_0 & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & \ldots & 0 & b_n & b_{n-1} & \ldots & b_1 & b_0
\end{pmatrix}$$

where the coefficients of f are repeated on n rows, and the coefficients of g are repeated on m rows.

Question 2 Show that f and g have a common root if and only if the Sylvester matrix is singular. (Hint: Consider dependence relations between the polynomials $f, xf, \ldots, x^{n-1}f$ and $g, xg, \ldots, x^{m-1}g$.) Compute the determinant of the Sylvester matrix for the examples in Question 1 and comment on the results.

We write ∂f for the degree of f. The resultant has the following properties.

$$\begin{array}{rcll} \mathrm{Res}(f,g) & = & (-1)^{\partial f \partial g}\,\mathrm{Res}(g,f) & \text{for } f,g \in \mathbb{C}[x], \\ \mathrm{Res}(\lambda f, \mu g) & = & \lambda^{\partial g}\mu^{\partial f}\,\mathrm{Res}(f,g), & \text{for } f,g \in \mathbb{C}[x] \text{ and } \lambda,\mu \in \mathbb{C}, \\ \mathrm{Res}(f,gh) & = & \mathrm{Res}(f,g)\,\mathrm{Res}(f,h) & \text{for } f,g,h \in \mathbb{C}[x], \\ \mathrm{Res}(f,g) & = & \mathrm{Res}(f,g+hf) & \text{for } f,g,h \in \mathbb{C}[x] \text{ with } f \text{ monic.} \end{array}$$

Question 3 Write a procedure that given polynomials $f, g \in \mathbb{Z}[x]$ (with g non-zero) computes $0 \neq c \in \mathbb{Z}$ and $q, r \in \mathbb{Z}[x]$ with $cf = qg + r$ and $\partial r < \partial g$. Then write a recursive procedure for computing the resultant of two polynomials in $\mathbb{Z}[x]$ using only integer arithmetic. Briefly describe how your program works.

Question 4 Show that for all but finitely many primes p, the following pairs of polynomials are coprime mod p, i.e. the polynomials obtained by reducing each coefficient mod p are coprime in $\mathbb{F}_p[x]$.

- $f_1(x) = x^3 - 3x^2 + 2x + 1$ and $g_1(x) = 2x^2 - x + 1$,
- $f_2(x) = x^3 + 4x^2 + 5x + 13$ and $g_2(x) = 3x^3 + 2x^2 + 4x - 9$,
- $f_3(x) = x^5 + x^2 - 9x + 25$ and $g_3(x) = 2x^3 + 7x^2 + 31x + 69$,
- $f_4(x) = x^6 + 7x^2 + x - 3$ and $g_4(x) = x^5 + 3x^2 + 31x + 10$.

In each case determine the finite set of exceptional primes.

The *discriminant* of $f(x) = \prod_{i=1}^{m}(x - \alpha_i)$ is $\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$.

Question 5 Find a formula for the discriminant in terms of a resultant.

3 Solving polynomial equations

The resultant can be defined more generally for polynomials with coefficients in any ring R. For instance R could itself be a polynomial ring.

Question 6 Write a program to compute the resultant of two polynomials with coefficients in $\mathbb{Z}[y]$. You should do this *either* by adapting your earlier programs *or* by using the fact that a polynomial of degree r is uniquely determined by any $r+1$ values. For the latter you will first need a bound on the degree of the answer as a polynomial in y.

Use your program to solve the following sets of polynomial equations.

$$\left\{ \begin{array}{rcl} 2x^2 - 2xy + 6x - 3y^2 + y + 4 & = & 0 \\ 3x^2 - 3x - 2y^2 - 6y - 4 & = & 0 \end{array} \right\}$$

$$\left\{ \begin{array}{rcl} 2x^2 + 3xy - x + 2y^2 - 2y - 4 & = & 0 \\ 5x^2 + 4xy + 4y^2 - 16 & = & 0 \end{array} \right\}$$

4 The Galois group of a polynomial

Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n, which we assume has no repeated roots. The Galois group of f is $\mathrm{Gal}(f) = \mathrm{Gal}(K/\mathbb{Q})$, where K is the splitting field of f. It acts by permuting the roots $\alpha_1, \ldots, \alpha_n$ of f, and hence is a subgroup of S_n.

Now let S_n act on the multivariate polynomial ring $P = \mathbb{Z}[X_1, \ldots, X_n]$ by permuting the indeterminates $X_1, \ldots, X_n$. Let $h_1, \ldots, h_m$ be the orbit of some multivariate polynomial $h \in P$ (with say $h_1 = h$) under this action and write $\mathrm{Stab}(h) \leqslant S_n$ for the stabilizer. The *resolvent* of f with respect to h is the polynomial

$$R_h(f) = \prod_{i=1}^{m} (x - h_i(\alpha_1, \ldots, \alpha_n)).$$

For example if $f(x) = x^4 + px^2 + qx + r$ and $h = -(X_1 + X_2)(X_3 + X_4)$ then

$$R_h(f) = x^3 + 2px^2 + (p^2 - 4r)x - q^2.$$

If $R_h(f)$ has distinct roots then it can be shown that $\mathrm{Gal}(f)$ is conjugate in S_n to a subgroup of $\mathrm{Stab}(h)$ if and only if $R_h(f)$ has an integer root.

Question 7 What does this construction tell us in the cases $h(X_1, \ldots, X_n) = X_1$ and $h(X_1, \ldots, X_n) = \prod_{i<j}(X_i - X_j)$?

We can use floating point approximations to exactly determine a number already known to be an integer, or to prove that a number is *not* an integer. (Strictly speaking we need to bound the rounding errors. Such an analysis is not expected for this project.) However it is in general impossible to *prove* that a number is an integer using floating point approximations.

Question 8 Write a program to compute the resolvent in the following cases. Your program should take as input a monic polynomial f with integer coefficients.

$$\begin{array}{ll} n = 4 & h = X_1X_2 + X_3X_4, \\ n = 4 & h = X_1X_2^2 + X_2X_3^2 + X_3X_4^2 + X_4X_1^2, \\ n = 5 & h = \sum_{i=1}^{5} X_i^2(X_{i+1}X_{i+4} + X_{i+2}X_{i+3}). \end{array}$$

In the third case the subscripts should be read as integers mod 5.

Question 9 Use the programs you have written for this project to investigate the Galois groups of the following irreducible polynomials. Why can you assume that they do not have repeated roots?

$$\begin{array}{ll} x^4 - 7x^2 - 6x + 1, & x^5 - x^3 - 7x^2 - x - 3, \\ x^4 - x^3 + 9x + 10, & x^5 - x^4 + 8x^2 - 7x + 3, \\ x^4 + 2x^3 + 23x^2 + 22x + 6, & x^5 - 2x^4 + 6x^3 - 3x^2 - x + 6. \end{array}$$

5 Programming

If you use MATLAB then you may wish to use the `DocPolynom` class that is included as an example in the help browser. To use this you should create a directory `@DocPolynom` and place `DocPolynom.m` into it. This will enable you to define and display (non-zero) polynomials and

to carry out standard algebraic manipulations with them (for instance adding, multiplying, evaluating). There is no need to include the class file in your program listings, assuming you do not modify it.

You may use inbuilt functions for integer arithmetic such as `gcd` and `factor`.

In Question 3 you are asked to write your own function, and so should not use the MATLAB function `deconv`.

