Resource A

The discriminant of a polynomial

A.1 Algebraic closure

You will be familiar with the Fundamental Theorem of Algebra: *a non-constant polynomial* $f(z) \in \mathbb{C}[z]$ *has a root* $\alpha \in \mathbb{C}$. It follows that $f(z)$ factorizes into linear factors:

$$f(z) = c(z - \alpha_1) \cdots (z - \alpha_n),$$

where $c, \alpha_1, \ldots, \alpha_n \in \mathbb{C}$.

In particular, a non-constant polynomial $f(x) \in \mathbb{R}[x]$ has a root $\alpha \in \mathbb{C}$. Conversely, any $\alpha \in \mathbb{C}$ satisfies a polynomial $f(x) \in \mathbb{R}[x]$, namely $f(x) = (x - \alpha)(x - \bar{\alpha})$. We say that $\mathbb{C}$ is the *algebraic closure* of $\mathbb{R}$, and write

$$\mathbb{C} = \overline{\mathbb{R}}.$$

In fact, every field k has an algebraic closure $\bar{k}$, ie a field with the properties

1. $\bar{k}$ is an extension of k, ie $k \subset \bar{k}$,
2. every non-constant polynomial $f(x) \in k[x]$ has a root in $\bar{k}$,
3. every $\alpha \in \bar{k}$ is the root of a polynomial $f(x) \in k[x]$.

Moreover, $\bar{k}$ is unique (up to isomorphism).

We shall assume this result without proof. (A short but difficult proof can be found in Wikipedia under "Algebraic closure".)

We are also going to assume a much simpler result, on symmetric polynomials. A polynomial $f(x_1, \ldots, x_n)$ over a field k (or more generally over a

commutative ring A) is said to be *symmetric* if it is left unchanged by any permutation of the variables, eg $x+y+z, xy+xz+yz, xyz$ are symmetric functions of x, y, z.

We know that if the polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

has roots $\alpha_1, \ldots, \alpha_n$, so that

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$$

then

$$\sum \alpha_i = -a_1 \sum_{i<j} \alpha_i\alpha_j = a_2, \sum_{i<j<k} \alpha_i\alpha_j\alpha_k = -a_3,$$

and so on.

The result asserts that every symmetric polynomial $f(\alpha_1, \ldots, \alpha_n)$ is expressible in terms of these so-called elementary symmetric polynomials. More precisely,

$$f(\alpha_1, \ldots, \alpha_n) = F(a_1, \ldots, a_n),$$

where $F(x_1, \ldots, x_n \in \mathbb{Z}[x_1, \ldots, x_n)$, ie F is a polynomial with integer coefficients. It follows in particular that

$$f(\alpha_1, \ldots, \alpha_n) \in k.$$

For example, if $n = 3$ then

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = a_1^2 - 2a_2.$$

(This is one of Newton's identities.)

A.2 The discriminant of a polynomial

Definition A.1 *A polynomial is said to be* separable *if it has distinct roots.*

Definition A.2 *The discriminant of a polynomial $f(x) \in k[x]$ with roots $\alpha_1, \ldots, \alpha_n$ is*

$$\Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

An alternative way of writing this is

$$\Delta(f) = (-1)^n \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Proposition A.1 *The polynomial $f(x)$ is separable if and only if $\Delta(f) \neq 0$.*

Lemma 21 *If $f(x) \in k[x]$ then $\Delta(f) \in k$.*

This follows from the fact that $\Delta(f)$ is a symmetric polynomial in the roots of f.

There is another approach to seperability.

Proposition A.2 *The polynomial $f(x)$ is separable if and only if* $\gcd(f(x), f'(x)) = 1$.

Here $f'(x)$ denotes the derivative of $f(x)$. Recall that the gcd (greatest common divisor) of $f(x)$ and $f'(x)$ can be computed by the euclidean algorithm.

Proposition A.3 *If $f(x) \in k[x]$ is a monic polynomial then*

$$\Delta(f) = (-1)^n \prod_{1 \leq i \leq n} f'(\alpha_i).$$

Proof ► On differentiating $f(x) = \prod(x - \alpha_i)$ and setting $x = \alpha_i$,

$$f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j).$$

Hence

$$\Delta(f) = \prod_i f'(\alpha_i).$$

◄

A.3 A special case

Proposition A.4 *Suppose $f(x) = x^3 + bx + x$. Then*

$$\Delta(f) = -(4b^3 + 27c^2)$$

Proof ► Let the roots of $f(x)$ be $\alpha_1, \alpha_2, \alpha_1$. Since $f'(x) = 3x^2 + b$,

$$\Delta(f) = - \prod_{1 \leq i \leq 3} (3\alpha_i^2 + b).$$

Thus if we set $A_i = 3\alpha_i^2 + b$ then

$$\Delta(f) = -A_1 A_2 A_3.$$

To find the cubic equation satisfied by the A_i, set $y = 3x^2 + b$. Then

$$3f(x) = x(y + 2b) + 3c.$$

Thus

$$f(x) = 0 \Longrightarrow x(y + 2b) = -3c.$$

Squaring,

$$f(x) = 0 \Longrightarrow x^2(y + 2b)^2 = 9c^2.$$

Multiplying by 3 and substituting for $3x^2$,

$$f(x) = 0 \Longrightarrow (y - b)(y + 2b)^2 = 27c^2.$$

So A_1, A_2, A_3 are roots of the cubic

$$y^3 + 3by^2 - (4b^3 + 27c^).$$

(We only need the constant term.) Hence

$$A_1A_2A_3 = 4b^3 + 27c^2,$$

and so

$$\Delta(f) = -(4b^3 + 27c^2).$$

◀

A.4 The resultant of two polynomials

The resultant, which is closely related to the discriminant, is used to determine if two polynomials have a root in common.

Definition A.3 *The resultant of two monic polynomials $f(x), g(x) \in k[x]$ with roots $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ is*

$$\mathrm{R}(f, g) = \prod_{i,j} (\alpha_i - \beta_j).$$

Proposition A.5 *The polynomials $f(x), g(x)$ have a root in common if and only if $\mathrm{R}(f, g) = 0$.*

Proposition A.6 *If $f(x), g(x) \in k[x]$ then $\mathrm{R}(f, g) \in k$.*

This follows from the fact that

$$\mathrm{R}(f, g) = \prod_i \left(\prod_j (\alpha_i - \beta_j) \right) = \prod_i g(\alpha_i).$$

Proposition A.7 $\Delta(f) = \mathrm{R}(f, f')$.

We saw that

$$\Delta(f) = \prod_i f'(\alpha_i).$$

Proposition A.8 *The resultant of the polynomials*

$$f(x) = x^m + a_1 x^{m-1} + \cdots + a_m,\ g(x) = x^n + b_1 x^{n-1} + \cdots + b_n$$

is given by

$$\mathrm{R}(f,g) = \det \begin{pmatrix} 1 & a_1 & a_2 & \cdots & a_m & 0 & \cdots & 0 \\ 0 & 1 & a_1 & a_2 & \cdots & a_m & \cdots & 0 \\ \cdots & & & & & & & \\ 1 & b_1 & b_2 & \cdots & b_n & 0 & \cdots & 0 \\ 0 & 1 & b_1 & b_2 & \cdots & b_n & \cdots & 0 \\ \cdots & & & & & & & \end{pmatrix}$$

This is known as the *Sylvester matrix* of f and g. It is an $(m+n)\times(m+n)$ matrix, with n rows filled with the coefficients of $f(x)$, successively shifted one column to the right, followed by m rows filled with the coefficients of $g(x)$, shifted similarly.

Suppose γ is a simultaneous root of f and g. If we multiply the columns of the matrix by $\gamma^{m+n-1}, \gamma^{m+n-2}, \ldots, 1$ and add, we see that all the sums vanish, and so the determinant vanishes. To complete the proof that determinant is in fact the resultant, see the Wikipedia entry for "Sylvester matrix".

Exercises 1 Discriminant

In exercises 1–6 determine the discriminant of the given polynomial.

* 1. $x^2 + bx + c$

* 2. $x^3 + 1$

** 3. $x^3 + x^2 + x$

** 4. $x^3 + x^2 + 1$

*** 5. $x^3 + ax^2 + bx + c$

** 6. $x^4 - 2$

*** 7. $x^5 + x^3 + 1$

In exercises 8–10 determine for what values of c the given polynomial is separable.

* 8. $x^2 + x + c$

** 9. $x^3 + x^2 + c$

** 10. $x^n - c$

** 11. Show that if a cubic polynomial $f(x) \in k[x]$ is not separable then all its roots are in k.

* 12. Show that a quadratic polynomial $f(x) \in \mathbb{R}[x]$ has 2 distinct real roots if and only if $\Delta(f) > 0$.
How many real roots does it have if $\Delta(f) < 0$

*** 13. Show that a cubic polynomial $f(x) \in \mathbb{R}[x]$ has 3 distinct real roots if and only if $\Delta(f) > 0$.
How many real roots does it have if $\Delta(f) < 0$

*** 14. Determine the number of real roots of $f(x) = x^4 + x + c$ for different values of c.

**** 15. Express the roots of a cubic polynomial $f(x)$ in terms of $\Delta(f)$.

*** 16. Show that $\mathrm{R}(f, g)$ is given by the Sylvester matrix.
Hence suggest a formula for $\Delta(f)$ when f is not necessarily monic.

In exercises 17–20 determine the resultant of the two given polynomials.

* 17. $x^2 + 1,\ 2x - 1$.

** 18. $x^3 + x^2 + 1,\ x^2 - 2$.

* 19. $x^2 + 1,\ 2x - 1$.

** 20. $x^4 + x + 1,\ x^2 + x + 1$.