2.2 Exercise Sheet 2

2.2.1 Numerical and Exploration

Exercise 2.2.1. Show that if k is any field of characteristic zero (e.g. $k = \mathbb{R}$ or $k = \mathbb{C}$), then the affine curve $C = C_f \subset \mathbb{A}^2_k$ defined by the vanishing of the polynomial

$$f(x, y) = y^2 - x^3 + x \in k[x, y]$$

cannot be parametrized by rational functions, using the following proof outline.

(a) Suppose to the contrary that it can, and use this to produce polynomials $f, g, h \in k[t]$ that satisfy all of the following properties simultaneously:

  (i) $h \neq 0$ and not all of f, g, h are constant,

  (ii) the polynomials f, g, h are coprime as a triple, i.e. that $(f, g, h) = (1)$ in $k[t]$, and

  (iii) $g^2h - f^3 + fh^2 = 0$.

(b) Verify the following matrix identities over the ring $k[t]$ (or equivalently field $K = k(t)$):

$$\begin{bmatrix} f & g & h \\ f' & g' & h' \end{bmatrix} \cdot \begin{bmatrix} -3f^2 + h^2 \\ 2gh \\ g^2 + 2fh \end{bmatrix} = \begin{bmatrix} f & g & h \\ f' & g' & h' \end{bmatrix} \cdot \begin{bmatrix} gh' - hg' \\ hf' - fh' \\ fg' - gf' \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Here f' denotes the formal derivative[4] of f with respect to t, and similarly for g' and h'.

(c) Show that the 2×3 matrix

$$\begin{bmatrix} f & g & h \\ f' & g' & h' \end{bmatrix}$$

has full rank, i.e. that at least one of $gh' - hg', hf' - fh', fg' - gf' \in k[t]$ is nonzero. (Hint: Exercise 2.2.11(a).)

(d) Use (b), (c), and basic linear algebra over the field $K = k(t)$ to conclude that there are relatively prime polynomials $p(t), q(t) \in k[t]$ with $q(t) \neq 0$ satisfying

$$q(t) \cdot \begin{bmatrix} -3f^2 + h^2 \\ 2gh \\ g^2 + 2fh \end{bmatrix} = p(t) \cdot \begin{bmatrix} gh' - hg' \\ hf' - fh' \\ fg' - gf' \end{bmatrix}. \tag{2.1}$$

(e) Show that the polynomials $-3f^2 + h^2, 2gh, g^2 + 2fh \in k[t]$ are coprime as a triple, i.e. in $k[t]$, we have that

$$(-3f^2 + h^2, 2gh, g^2 + 2fh) = (1).$$

Conclude that $p(t)$ is a nonzero constant.

(f) Use the equation (a)(iii) and the matrix equation (2.1) to derive a contradiction. (Hint: do some case-work on the possible relationships between the degrees of f, g and h.)

(g) Why do the polynomials $-3f^2 + h^2, 2gh$ and $g^2 + 2fh$ show up in this proof? What goes wrong in the above proof if you try to repeat it for $f(x, y) = y^2 - x^3 - x^2 \in k[x, y]$ instead? (We showed in Example 1.3.7 that this curve admits a rational parametrization.)

(h) Where in the proof did you use $\operatorname{ch} k = 0$? Investigate what happens in positive characteristic. Is the result still true? If not, can you come up with a parametrization? If yes, then does the same proof work? If the result is true but the proof doesn't work, can you come up with a different proof?

This proof due to Kapferer has been adapted from [2]. With minor modifications, the same proof shows that any over a field k with $\operatorname{ch} k = 0$, every smooth projective curve of degree at least 3 cannot be parametrized by rational functions. In modern algebraic geometry, this is often seen as a consequence of the Riemann-Hurwitz formula.[5]

[4] If you haven't seen this notion before, then define it.

[5] If you know what that is, do you see why this result is a consequence of it?

Exercise 2.2.2. Let $C_e \subset \mathbb{A}^2_{\mathbb{R}}$ denote the Cassini curve of eccentricity $e \in (0, \infty)$ (see Example 1.2.12). For concreteness, you may take $C_e := C_{f_e}$, where

$$f_e(x, y) := \left((x-1)^2 + y^2\right)\left((x+1)^2 + y^2\right) - e^4 \in \mathbb{R}[x, y].$$

Show that:

(a) The curve C_e consists of two pieces[6] if $0 < e < 1$ and one piece if $e \geq 1$.
(b) The curve C_e is smooth[7] if and only if $e \neq 1$.
(c) For $e > 1$, the unique oval in C_e is convex[8] iff $e \geq \sqrt{2}$.

Exercise 2.2.3 (More Parametric Curves). Using the proof strategy from Example 1.3.10 and Remark 1.3.11 or otherwise, come up with Cartesian equations defining the parametric curves given by the following parametrizations.

(a) $(t^4 + 2t - 3, t^3 + 2t^2 - 5)$
(b) $\left(\dfrac{t(t^2+1)}{t^4+1}, \dfrac{t(t^2-1)}{t^4+1}\right)$

Now come up with a few examples of your own devising, and repeat the same. Can you write a program that does these (somewhat tedious) calculations for you?

Exercise 2.2.4 (Resultants). For those who know a little linear algebra, this exercise provides a different perspective on the resultant of two polynomials than is presented in the Ross set on this topic (which you should now solve if you haven't done so previously!).

For a field K and for each integer $N \geq 0$, let $K[t]_N \subset K[t]$ denote the subspace of polynomials of degree strictly less than N, so that $\dim_K K[t]_N = N$. Given polynomials $f, g \in K[t]$ of degree $m, n \geq 0$ respectively, we can investigate whether or not f and g have a common factor in $K[t]$ as follows.

(a) Consider the linear map $\phi : K[t]_n \times K[t]_m \to K[t]_{m+n}$ given by $\phi(u, v) := uf + vg$. Show that f and g have a common factor in $K[t]$ of positive degree iff the map ϕ is not injective. (Hint: use that $K[t]$ is a UFD.)
(b) Show that if we choose the ordered basis

$$(t^{n-1}, 0), (t^{n-2}, 0), \ldots, (1, 0), (0, t^{m-1}), (0, t^{m-2}), \ldots, (0, 1)$$

of the domain and

$$t^{m+n-1}, t^{m+n-2}, \ldots, 1$$

of the range, then the matrix representative of ϕ with respect to these bases is

$$\mathrm{Syl}(f, g) := \begin{bmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 \\ a_m & a_{m-1} & \cdots & \vdots & b_n & b_{n-1} & \cdots & \vdots \\ 0 & a_m & \ddots & \vdots & 0 & b_n & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_{m-1} & \vdots & \vdots & \ddots & b_{n-1} \\ 0 & 0 & \cdots & a_m & 0 & 0 & \cdots & b_n \end{bmatrix},$$

where $f(x) = a_0 t^m + \cdots + a_m$ and $g(x) = b_0 t^n + \cdots + b_n$. This matrix is called the Sylvester matrix of f and g.

[6] Here the word "piece" means "connected component".
[7] What does that mean?
[8] What does that mean?

(c) The determinant of the Sylvester matrix of f and g is called the called the resultant of f and g with respect to t, often written $\mathrm{Res}_t(f, g)$ or simply $\mathrm{Res}(f, g)$, so that

$$\mathrm{Res}(f, g) := \det \mathrm{Syl}(f, g) \in \mathbb{Z}[a_0, \dots, a_m, b_0, \dots, b_n] \subset K.$$

Show, using some basic linear algebra, that f and g share a common factor in $K[t]$ iff

$$\mathrm{Res}(f, g) = 0 \in K.$$

(Hint: the domain and range of ϕ have the same dimension over K.)

(d) Conclude that if K is algebraically closed and $a_0 b_0 \neq 0$, then f and g have a common root $t = t_0 \in K$ iff

$$\mathrm{Res}(f, g) = 0.$$

(What happens if $a_0 b_0 = 0$?) Use this to show that, even if K is not algebraically closed, and $\alpha_1, \dots, \alpha_m$ and $\beta_1, \dots, \beta_n$ are roots of f and g, respectively, in some extension field $K' \supset K$ of K, then

$$\mathrm{Res}(f, g) = a_0^n b_0^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) = a_0^n \prod_{i=1}^{m} g(\alpha_i) = (-1)^{mn} b_0^m \prod_{j=1}^{n} f(\beta_j).$$

(e) Let's do one example computation: show that if $m = n = 2$ and

$$f(t) = a_1 t^2 + b_1 t + c_1 \text{ and}$$
$$g(t) = a_2 t^2 + b_2 t + c_2,$$

then

$$\mathrm{Res}(f, g) = (a_1 c_2 - a_2 c_1)^2 - (a_1 b_2 - a_2 b_1)(b_1 c_2 - b_2 c_1).$$

In particular, these quadratic equations have a common root (in K, or if necessary, a quadratic extension of K) iff this polynomial of degree 4 in the coefficients vanishes.

(f) Finally, let's use this notion of resultants to complete the computation begun in Example 1.3.10. In the notation of Example 1.3.10, show that if the base field k is algebraically closed, then $C = C_f$, i.e. our parametrization gives us the complete curve C_f.

Exercise 2.2.5 (Discriminants). Given a field K and a polynomial $f(t) \in K[t]$, the discriminant of f, written $\mathrm{disc}(f)$, is the resultant of f and its (formal) derivative f' with respect to t, up to scalar factors. More precisely, if $f(t) = a_0 t^m + \cdots + a_m$ with $a_j \in K$ and $a_0 \neq 0$, then we define

$$\mathrm{disc}(f) := \frac{(-1)^{m(m-1)/2}}{a_0} \cdot \mathrm{Res}(f, f').$$

Let's do a few examples.

(a) Show that if $f(t) = at^2 + bt + c$, with $a \neq 0$, then $\mathrm{disc}(f) = b^2 - 4ac$.

(b) Show that if $f(t) = t^3 + pt + q$, then $\mathrm{disc}(f) = -4p^3 - 27q^2$. How does this relate to Exercise 2.1.4?

(c) Show that if over an extension field $K' \supset K$, the polynomial f splits into linear factors as

$$f(t) = a_0 \prod_{i=1}^{m} (t - \alpha_i) \in K'[t]$$

for some $\alpha_i \in K'$, then

$$\mathrm{disc}(f) = a_n^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j).$$

(d) Show that the polynomial $f(t)$ has a repeated root over an algebraic closure of K iff $\mathrm{disc}(f) = 0$. In other words, if there is an α some extension field $K' \supset K$ and a polynomial $q(t) \in K'[t]$ such that

$$f(t) = (x - \alpha)^2 q(t),$$

then $\mathrm{disc}(f) = 0$, and conversely, if $\mathrm{disc}(f) = 0$, then we can find such α, K and q.

2.2.2 PODASIPs

Prove or disprove and salvage if possible the following statements.

Exercise 2.2.6. For a field k, let $\mathrm{Fun}(\mathbb{A}^2_k, k)$ be the set of all functions $F : \mathbb{A}^2_k \to k$. Claim: for any field k, the map

$$k[x,y] \to \mathrm{Fun}(\mathbb{A}^2_k, k), \quad f \mapsto F_f$$

which sends a polynomial to the corresponding polynomial function is injective. In other words, if two polynomials $f, g \in k[x,y]$ agree at all points $(p,q) \in \mathbb{A}^2_k$, then $f = g$.

Exercise 2.2.7. If k is any infinite field and $C \subset \mathbb{A}^2_k$ an algebraic curve, then the complement

$$\mathbb{A}^2_k \smallsetminus C$$

of C in $\mathbb{A}^2_k$ is infinite.

Exercise 2.2.8. A field is algebraically closed if and only if it is infinite.

Exercise 2.2.9. For any field k, if $f, g \in k[t]$ are polynomials such that

$$f(t)^2 + g(t)^2 = 1$$

as polynomials, then $f(t)$ and $g(t)$ are constant. In other words, the "unit circle" $C \subset \mathbb{A}^2_k$ does not admit a polynomial parametrization.

Exercise 2.2.10 (Separability). For any field K and polynomial $f(t) \in K[t]$, we say that f is separable if an algebraic closure of K separates the roots of f, i.e. that $\mathrm{disc}(f) \neq 0 \in K$. (See Exercise 2.2.5.) Claim: for any field K and $f(t) \in K[t]$, the polynomial f is separable if and only if it is irreducible as an element of the ring $K[t]$.

Exercise 2.2.11 (Wronskians).

(a) For any field k and polynomials $f, g \in k[t]$ in one variable t over k, we have $fg' = gf'$ iff there are $\alpha, \beta \in k$, not both zero, such that $\alpha f + \beta g = 0$. Here, as before, f' (resp. g') denotes the formal derivative of f (resp. g) with respect to t.

(b) More generally, for any field k, integer $n \geq 1$, and polynomials $f_1, \ldots, f_n \in k[t]$ in one variable t over k, the determinant

$$W(f_1, \ldots, f_n) = \det \begin{bmatrix} f_1 & f_2 & \cdots & f_n \\ f_1' & f_2' & \cdots & f_n' \\ \vdots & \vdots & \ddots & \vdots \\ f_1^{(n-1)} & f_2^{(n-1)} & \cdots & f_n^{(n-1)} \end{bmatrix} \in k[t]$$

vanishes (i.e. we have $W(f_1, \ldots, f_n) = 0$ as a polynomial) iff the $f_1, \ldots, f_n \in k$ are linearly dependent, i.e. there are $\alpha_1, \ldots, \alpha_n \in k$, not all zero, such that

$$\alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_n f_n = 0.$$

Here, for any $f \in k[t]$ and $j \geq 0$, the symbol $f^{(j)}$ denotes the j^{th} formal derivative of f with respect to t, so that $f^{(0)} = f$ and we have $f^{(1)} = f'$, $f^{(2)} = f''$, etc.