Algebraic Curves: Worksheet 2

Parametrisations, Nullstellensatz

	D	C	B	B+/A-	A
γ	all	all	all	all	all
β	0	1	1	2	2
α	0	0	1	1	2

γ **Exercise 1.** For any subset $X \subset k^n$, define $\mathbb{I}(X) \subset k[x_1, \ldots, x_n]$ by

$$\mathbb{I}(X) = \{f \in k[x_1, \ldots, x_n] \,:\, f(p) = 0 \ \forall p \in X\}.$$

For any set S of polynomials, define $\mathbb{V}(S) \subset k^n$ by

$$\mathbb{V}(S) = \{x \in k^n \,:\, f(x) = 0 \text{ for all } f \in S\}$$

(a) Show that $\mathbb{I}(X)$ is an ideal.

(b) Show that if $X \subset Y$ then $\mathbb{I}(Y) \subset \mathbb{I}(X)$.

(c) Show that if $S \subset T$ then $\mathbb{V}(T) \subset \mathbb{V}(S)$.

To promote this to a β-question, try writing your proofs using words and sentences instead of just relying on symbols.

γ **Exercise 2.** By looking at the line $x = ty$ with slope $1/t$, passing through the origin, find a rational (in fact, polynomial) parametrisation of $xy^2 - 6x^3 = y^4$.

γ **Exercise 3.** All of the following statements are false: give counterexamples.

(a) Every maximal ideal of $\mathbb{R}[x]$ is of the form $(x - a)$ for some $a \in \mathbb{R}$.

(b) If I is a maximal ideal in $\mathbb{R}[x]$ then $\mathbb{R}[x]/I = \mathbb{R}$.

(c) For any $f \in \mathbb{R}[x]$, if $g \in \mathbb{R}[x]$ vanishes at every point where f vanishes then $g^r \in (f)$ for some r.

γ **Exercise 4.** Let $f(x, y) = (x-1)^2 + y^2 - 1$ and $g(x, y) = y^2 - x^3$. Find the intersection $\{f = 0\} \cap \{g = 0\}$.

β **Exercise 5.** Recall that

$$K(m) = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-mx^2)}}.$$

Using the substitution $\xi = \frac{1}{\sqrt{1-(1-m)x^2}}$, show that

$$K(1-m) = \int_1^{1/\sqrt{m}} \frac{d\xi}{\sqrt{(\xi^2-1)(1-m\xi^2)}}.$$

Using the substitution $\eta = \frac{1}{x\sqrt{m}}$, show that

$$\int_{1/\sqrt{m}}^{\infty} \frac{d\eta}{\sqrt{(1-\eta^2)(1-m\eta^2)}} = K(m).$$

β **Exercise 6.** Let R be a ring and $I \subset R$ an ideal. Let $q\colon R \to R/I$ be the quotient map. We call an ideal J *intermediate* if $I \subset J \subset R$. Show that

$$J \mapsto q(J)$$

defines a bijection between intermediate ideals and ideals of the quotient ring R/I.

β **Exercise 7.** Let k be an algebraically closed field. Assuming the weak Nullstellensatz, show that the only maximal ideals in $k[x_1, \ldots, x_n]$ are those of the form $(x_1 - a_1, \ldots, x_n - a_n)$. (Hint: If I is a maximal ideal and $\boldsymbol{a} \in \mathbb{V}(I)$, show that $I \subset \mathfrak{m}_{\boldsymbol{a}}$).

β **Exercise 8.** Building on Exercise 1:

(a) For any set S of polynomials, show that $S \subset \mathbb{I}(\mathbb{V}(S))$.

(b) For any set $X \subset k^n$, show that $X \subset \mathbb{V}(\mathbb{I}(X))$.

(c) Show that

$$\mathbb{V}(\mathbb{I}(\mathbb{V}(S))) = \mathbb{V}(S) \text{ and } \mathbb{I}(\mathbb{V}(\mathbb{I}(X))) = \mathbb{I}(X)$$

for any set S of polynomials and any subset $X \subset k^n$.

(d) Show that two algebraic sets V_1, V_2 are equal if and only if $\mathbb{I}(V_1) = \mathbb{I}(V_2)$.

α **Exercise 9.** Fix an integer c and consider the curve $C = \{x^3 + y^2 = c\}$. Integer points on C correspond to ways of writing c as a sum of a square and a cube or a difference of a square and a cube. For example, $1^3 + 4^2 = 2^3 + 3^2 = (-2)^3 + 5^2 = 17$. Here are two ways of generating more $\mathbb{Q}$-points on a cubic like this:

- Take the straight line connecting two $\mathbb{Q}$-points p, q and look for its third point of intersection with C (a generic line and a cubic intersect at three points).

- Take a tangent line[1] to C at a $\mathbb{Q}$-point p and look for its third point of intersection with C.

What weird and wonderful new solutions of $x^3 + y^2 = 17$ can you generate like this? (Stop when you start generating solutions with x, y rational and non-integer. You may use a computer if you can figure out how!)

Remark: Underpinning this amazing strategy for generating $\mathbb{Q}$-points is a special abelian group called the Mordell-Weil group. It is the set of $\mathbb{Q}$-points together with a point (the identity) at infinity; the group operation is defined in such a way that $p + q + r = 0$ precisely when p, q, r lie on a line.

α **Exercise 10.** Recall that the units in a commutative unital[2] ring are the invertible elements, i.e. the elements a for which there exists a b with $ab = 1$. Let k be a field. What are the units in $k[x]$? In $k[x, y]$?

α **Exercise 11.** Let k be an algebraically closed field. In this question, we will prove the Nullstellensatz from the weak Nullstellensatz, using a trick due to Rabinowitz. Suppose that $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ generate our ideal I and suppose that $g \in k[x_1, \ldots, x_n]$ vanishes on $\mathbb{V}(I)$. Introduce a new variable x_0 and consider the ideal

$$J = (f_1, \ldots, f_n, x_0 g - 1) \subset k[x_0, \ldots, x_n].$$

(a) Show that $\mathbb{V}(J) = \emptyset \subset k^{n+1}$.

(b) Deduce that there exist polynomials $\alpha_1, \ldots, \alpha_n, \beta \in k[x_0, \ldots, x_n]$ such that

$$1 = \sum \alpha_i f_i + \beta(x_0 g - 1).$$

(c) Substitute $x_0 = 1/g$ and multiply both sides by a large power of g to ensure that the denominators of all the coefficients $\alpha_i(1/g, x_1, \ldots, x_n)$ have no factors of g. Why can you deduce that $g^N \in I$ for some N?

α **Exercise 12.** Let n be a positive integer. Suppose that there are non-constant polynomial functions $p(t), q(t), r(t) \in k[t]$ which are pairwise coprime and such that

$$p(t)^n + q(t)^n = r(t)^n. \tag{1}$$

Write p', q', r' for their derivatives and let $a = p^{n-1}, b = q^{n-1}, c = r^{n-1}$, so that we can write Equation 1 as $pa + qb = rc$.

(a) Prove that $p'a + q'b = r'c$.

(b) Deduce that there is a polynomial $s \in k[t]$ with

$$sa = qr' - q'r, \qquad sb = rp' - r'p, \qquad sc = p'q - pq'.$$

[1] The slope of the tangent line to $\{f = 0\}$ is $-\frac{\partial f/\partial x}{\partial f/\partial y}$.

[2] "Unital" just means there is an element 1 which behaves the way you want.

(c) Write $S = \deg(s)$, $A = \deg(a)$, etc. Show that $(n-3)(A+B+C) \leq -3(1+S)$.

(d) Deduce that $n \leq 2$ (Hint: $A = (n-1)P$, etc).

(e) Why does this prove that the curve $x^n + y^n = 1$ is not rational for any $n \geq 3$?
