

MATH 499: Homework 4

September 17, 2009

1. In each part, determine whether the polynomial f is in the given ideal I . Notice that determining if f lies in the ideal $\langle g \rangle$ is equivalent to determining if g divides f . How do we use the same idea in (c) and (d), where $I = \langle g_1, g_2 \rangle$?

(a) $f(x) = x^2 - 3x + 2, \quad I = \langle x - 2 \rangle$

(b) $f(x) = x^5 - 4x + 1, \quad I = \langle x^3 - x^2 + x \rangle$

(c) $f(x) = x^2 - 4x + 4, \quad I = \langle x^4 - 6x^2 + 12x - 8, 2x^3 - 10x^2 + 16x - 8 \rangle$

(d) $f(x) = x^3 - 1, \quad I = \langle x^9 - 1, x^5 + x^3 - x^2 - 1 \rangle$

2. Find an ideal $I \subset R[x]$ in which every element $f \in I$ is divisible by x , but such that $x \notin I$.
3. Recall that a rational function $x(t)$ is one of the form $x(t) = \frac{p(t)}{q(t)}$, where p and q are polynomials. Show that the following curves are rational by finding non-constant functions $x(t)$ and $y(t)$ such that $f(x(t), y(t)) \equiv 0$. Then use a computer to graph the curve from the implicit function and then from the parametrization to verify that they coincide (at least for some section of the curve).

Hint: Try using a substitution such as $t = \frac{y}{x}$ or $t = \frac{y}{x^2}$.

(a) $f(x, y) = y^2 - x^3$

(b) $f(x, y) = x^2 - y^2 - (x - 2y)(x^2 + y^2)$

(c) $f(x, y) = x^5 - xy^2 + y^3$

(d) $f(x, y) = 3x - 2y - y^2$

(e) $f(x, y) = x^5 - x^4 + x^2y - y^2$

(f) $f(x, y) = x^2 + 2xy + y^2 - y$

(g) $f(x, y) = x^2 - 2x - y + 1$

4. A *cardioid* is defined by the polar equation $r = 1 - \cos \theta$. Find an implicit polynomial equation $f(x, y) = 0$ for the cardioid, and show that

$$(x(t), y(t)) = ((\cos t)(1 - \cos t), (\sin t)(1 - \cos t))$$

is a (non-rational) parametrization of it.

5. Recall the definition of an affine equivalence from last week. Show that affine equivalence preserves rationality. That is, show that if $f(x, y) = g(\phi(x, y))$ for some affine equivalence ϕ and $V(g) = \{(x, y) : f(x, y) = 0\}$ is rational then $V(f)$ is also rational.
6. (a) Show that any conic is affine equivalent to one with no constant term, i.e. a conic of the form $f(x, y) = ax + by + cx^2 + dxy + ey^2$.

- (b) Let $f(x, y) = (ax + by) + (cx^2 + dxy + ey^2) = f_1 + f_2$ be irreducible, where f_i is the purely degree i part of the polynomial. Prove that $V(f)$ is rational.
- (c) Show that any irreducible conic is rational.
- (d) Now, let $f(x, y)$ be an irreducible degree n polynomial such that $f = f_{n-1} + f_n$, so that f has no terms of degree less than $n - 1$. Prove that $f(x, y) = 0$ is a rational curve.

7. On the last homework, we began investigating the solution of equations like $n = 4x + 6y$ and $n = 5x + 8y$. We discovered that which numbers are expressible in the form $ax + by$ for x, y integers seems to have a lot to do with the the greatest common divisor of a and b .

In fact, it turns out that the standard method of computing the g.c.d. d of a and b can help us solve the equation $d = ax + by$ for integers x and y . This computational method is called “Euclid’s algorithm” and works by repeated division with remainder as follows:

$$\begin{aligned}
 b &= q_1 a & + r_1 \\
 a &= q_2 r_1 & + r_2 \\
 r_1 &= q_3 r_2 & + r_3 \\
 &\dots \\
 r_{n-2} &= q_n r_{n-1} & + r_n \\
 r_{n-1} &= q_{n+1} r_n & + 0
 \end{aligned}$$

The algorithm eventually terminates when it gets a zero remainder (since the remainders get smaller at each step). At that point the g.c.d. of a and b is known to be the last non-zero remainder r_n .

- (a) Why does Euclid’s algorithm work to find the g.c.d.? [Hint: The common divisors of r_1 and r_2 are the same as the common divisors of r_2 and r_3 . (Why?)]
- (b) How does Euclid’s algorithm allow us to write the g.c.d. r_n in the form $ax + by$? Use it to solve $68x + 173y = 1$.
- (c) In the integers modulo 173, what is the multiplicative inverse of 68?