HW 4
Prof. Shahed Sharif

Homework due 9/27: 1.5/12, 13–16; 2.1/1, 5; 2.2/7

1.5.14ab For (a), we first show the usual derivative formula for $(x-a)^r$. By the Binomial Theorem (which holds over all fields),

$$(x-a)^r = \sum_{i=0}^{r} \binom{r}{i} x^{r-i} a^i.$$

Taking the derivative, we get

$$\begin{aligned}
\frac{d}{dx}(x-a)^r &= \sum_{i=0}^{r} \binom{r}{i} \cdot i \cdot x^{r-i} a^{i-1} \\
&= \sum_{i=1}^{r} \frac{r \cdot (r-1) \cdots (r-i+1)}{i!} \cdot i \cdot x^{r-i} a^{i-1} \\
&= \sum_{i=1}^{r} r \frac{(r-1) \cdot (r-2) \cdots ((r-1)-(i-1)+1}{(i-1)!} x^{(r-1)-(i-1)} a^{i-1} \\
&= r \sum_{j=0}^{r-1} \binom{r-1}{j} x^{(r-1)-j} a^j,
\end{aligned}$$

where $j = i-1$. Again via Binomial Theorem, the last expression is $r(x-a)^{r-1}$.

Next we get

$$\begin{aligned}
f' &= r(x-a)^{r-1} h + (x-a)^r h' \\
&= (x-a)^{r-1}(rh + (x-a)h').
\end{aligned}$$

Let $h_1 = rh + (x-a)h'$. We have

$$h_1(a) = rh(a) + 0 \neq 0$$

as $h(a) \neq 0$. The claim follows.

For (b), let $h_i = \frac{f}{(x-a_i)^{r_i}}$. Observe that $h_i(a_i) \neq 0$. By (a),

$$f' = (x-a_i)^{r_i - 1} H_i$$

for some H_i, $H_i(a_i) \neq 0$. In particular, $(x-a_i) \nmid H_i$. Observe that $x - a_i$ is irreducible, since all linear polynomials are irreducible. Since we have unique prime factorization in $k[x]$, $(x-a_i)^{r_i} \nmid f'$. We have

$$\frac{1}{a_j - a_i}[(x-a_i) - (x-a_j)] = 1$$

for $i \neq j$, and hence $\gcd(x - a_i, x - a_j) = 1$. Thus the linear polynomials are pairwise coprime irreducibles. The result follows from unique prime factorization.

2.1.1 For (a) and (b), we can just use % in Sage. The remainder in (a) is 0, so $f \in I$. In (b), the remainder is $-x^2 - 4x + 1$, so $f \notin I$.

For (c) and (d), we first need to compute the gcd of the generators of I, and then compute the remainder with the gcd as in (a) and (b). In (c), the gcd is 1, so $f \in I$ since I is the unit ideal. For (d), the gcd is $x - 1$, which clearly divides $x^3 - 1$. Thus $f \in I$ in this case as well.

2.1.5ab For part (a), the monomials of degree m are those of the form

$$x^0y^m, x^1y^{m-1}, x^2y^{m-2}, \dots, x^my^0.$$

Clearly there are $m + 1$ of these. The number of monomials of degree m is the sum of the number of monomials of degree i as i ranges in $0 \leq i \leq m$, yielding the sum

$$\sum_{i=0}^{m}(i+1).$$

This is the $(m+1)$st triangular number $\binom{m+2}{2}$, yielding the desired formula.

For (b), since $\binom{m+2}{2}$ grows quadratically in m while $nm + 1$ is linear in m, $\exists m$ such that

$$\binom{m+2}{2} \geq nm + 1.$$

Choose such an m. Let V be the vector space of polynomials of degree $\leq nm$. We have $\dim V = nm + 1$. The argument in (a) with f in place of x and g in place of y shows that there are $\binom{m+2}{2}$ expressions of the form f^ag^b with $a + b \leq m$. The list of polynomials $(f^ag^b)_{a+b\leq m}$ lies in V. Since the number of elements in this list is greater than the dimension of V, the list must be linearly dependent; thus, $\exists c_{a,b} \in k$ not all 0 such that

$$\sum_{a+b\leq m} c_{a,b}f^ag^b = 0$$

in $k[t]$. In particular, that means every point in C satisfies the polynomial equation

$$\sum_{a+b\leq m} c_{a,b}x^ay^b = 0.$$