Homework 3

*Algorithms for Elementary Algebraic Geometry*

Math 191, Fall Quarter 2007

Solutions.

1. Here is an algorithm to solve the ideal membership problem in $k[x]$:

   Let polynomials $f$ and $f_1, \ldots, f_s$ in $k[x]$ be given. Compute a greatest common divisor $g$ of $f_1, \ldots, f_s$ using the Euclidean Algorithm. If $g$ divides $f$, then output “$f \in \langle f_1, \ldots, f_s \rangle$”; otherwise output “$f \not\in \langle f_1, \ldots, f_s \rangle$.” (This is justified by $\langle g \rangle = \langle f_1, \ldots, f_s \rangle$.) Now we use this procedure and Maple to decide whether in $\mathbb{Q}[x]$ we have

   $x^2 - 4 \in \langle x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2 \rangle$.

   First we compute

   ```
   > gcd(x^3+x^2-4*x-4, x^3-x^2-4*x+4);
   2
   x - 4
   ```

   and then

   ```
   > gcd(x^2-4, x^3-2*x^2-x+2);
   x - 2
   ```

   Hence

   $g = \text{GCD}(x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2) = x - 2,$

   and since $g$ divides $f = x^2 - 4 = (x + 2)(x - 2)$, we see that $f$ lies in the ideal in question.

2. Our trusted companion Maple gives us:

   ```
   > gcd(x^3-1, x^6-1);
   3
   x - 1
   > gcd(x^19-1, x^7-1);
   x - 1
   > gcd(x^99-1, x^27-1);
   9
   x - 1
   ```

   Hence we are tempted to conjecture that in general,

   $$
   \text{GCD}(x^m - 1, x^n - 1) = x^d - 1
   $$

   where $d > 0$ is the greatest common divisor of the integers $m$ and $n$. 

3. Let $f \in \mathbb{C}[x]$, $f \neq 0$.

(a) The proof is by induction on $d = \deg(f)$. If $\deg(f) = 0$, then $f$ is a constant, so $f = c$ is a factorization of the desired form. Suppose that $d > 0$ and the claim is true for all polynomials of degree less than $d$. Assume that $f$ has degree $d$. By the Fundamental Theorem of Algebra, if $f$ is non-constant, $f$ has a zero, say $a$, in $\mathbb{C}$: $f(a) = 0$.

Now the Division Algorithm yields that

$$f(x) = g(x)(x-a) + r(x),$$

where $r = 0$ or $\deg(r) < \deg(x-a) = 1$, so $r$ is a constant. Thus

$$0 = f(a) = g(a)(a-a) + r,$$

which implies that $f = (x-a)g$. Since $d = \deg(f) = \deg(g) + \deg(x-a) = \deg(g) + 1 > \deg(g)$, by inductive hypothesis applied to $g$, there is a factorization of $g$ in the form

$$g = c(x-a_1)^{r_1} \cdots (x-a_m)^{r_m},$$

where $c \in \mathbb{C}$ is nonzero, and $a_1, \ldots, a_m$ are pairwise distinct. So

$$f = c(x-a)(x-a_1)^{r_1} \cdots (x-a_m)^{r_m}.$$

If $a, a_1, \ldots, a_m$ are pairwise distinct, this is a factorization of $f$ in the required form. If $a = a_i$ for some $i$ then

$$f = c(x-a_1)^{r_1} \cdots (x-a_i)^{r_i+1} \cdots (x-a_m)^{r_m}$$

is the desired factorization.

[Note that there was still another small inaccuracy in how the problem was formulated: instead of $r_1, \ldots, r_m$ non-negative, they should be required to be positive!]

(b) Clearly if $a \in \{a_1, a_2, \ldots, a_m\}$, then $f(a) = 0$. If $a \notin \{a_1, \ldots, a_m\}$ then $f(a) = c(a-a_1)^{r_1} \cdots (a-a_m)^{r_m}$ is the product of nonzero elements of $\mathbb{C}$, so is nonzero. Thus $V(f) = \{a_1, a_2, \ldots, a_m\}$.

(c) Since $f_{\text{red}}(a_i) = 0$ for $1 \leq i \leq m$, we have $f_{\text{red}} \in I(V(f))$. For the reverse inclusion, let $g \in I(V(f))$. Then $g(a_i) = 0$ for $1 \leq i \leq m$. We claim that $g$ is a multiple of $f_{\text{red}}$. The proof is by induction on the size $m$ of $V(f)$. If $m = 1$, then $f_{\text{red}} = x - a_1$, and the Division Algorithm implies that that

$$g = g(x-a_1) + r,$$

where $r$ is a constant; the fact that $g(a_1) = 0$ means that $r = 0$, so $g$ is a multiple of $x - a_1$. Now suppose that the claim is true if $V(f) < m$. The polynomial

$$f_1 := (x-a_1) \cdots (x-a_{m-1})$$
satisfies \( V(f_1) = \{a_1,\ldots,a_{m-1}\} \); hence we have \( I(V(f_1)) = \langle f_1 \rangle \) since \((f_1)_{\text{red}} = f_1\). Since \(g(a_i) = 0\) for \(1 \leq i \leq m - 1\), we know that \(g = f_1h\) where \(h \in \mathbb{C}[x]\). Since \(g(a_m) = 0\) but \(f_1(a_m) = (a_1 - a_m) \cdots (a_m - a_{m-1}) \neq 0\), we must have \(h(a_m) = 0\), and so by the base case \(h = (x - a_m)p\) for some \(p \in \mathbb{C}[x]\). Thus

\[
g = f_1h = (x - a_1)\ldots(x - a_{m-1})(x - a_m)p
\]

is a multiple of \(f_{\text{red}}\). This shows that \(I(V(f)) \subseteq \langle f_{\text{red}} \rangle\), and so the two ideals are equal.

(d) One first checks by computation that the operation \(p \mapsto p'\) satisfies the usual properties of the derivative: for all \(p,q \in \mathbb{C}[x]\) we have

\[
(p + q)' = p' + q', \quad (pq)' = p'q + pq' \quad \text{(Product Rule)}.
\]

This implies that \((p^n)' = np^{n-1}p'\) for every positive integer \(n\) and \(p \in \mathbb{C}[x]\). (I omit some details here.) Now applying the product rule to

\[
f = c(x - a_1)^{r_1}\cdots(x - a_m)^{r_m}
\]

we obtain

\[
f' = cr_1(x - a_1)^{r_1-1}(x - a_2)^{r_2}\cdots(x - a_m)^{r_m} + \\
    cr_2(x - a_1)^{r_1}(x - a_2)^{r_2-1}\cdots(x - a_m)^{r_m} + \cdots + \\
    cr_m(x - a_1)^{r_1}\cdots(x - a_2)^{r_2}\cdots(x - a_m)^{r_m-1}
\]

\[
= c(x - a_1)^{r_1}\cdots(x - a_m)^{r_m} \left( \frac{r_1}{x - a_1} + \cdots + \frac{r_m}{x - a_m} \right)
\]

\[
= c(x - a_1)^{r_1-1}\cdots(x - a_m)^{r_m-1}H(x)
\]

where

\[
H = (x - a_1)\cdots(x - a_m) \left( \frac{r_1}{x - a_1} + \cdots + \frac{r_m}{x - a_m} \right).
\]

Then \(H\) is a polynomial (why?) such that \(H(a_i) \neq 0\) for any \(i\). This implies that

\[
\text{GCD}(f,f') = (x - a_1)^{r_1-1}\cdots(x - a_m)^{r_m-1}.
\]

(e) This follows from (a) and (d). [Note that strictly speaking, this equation is only true “up to multiplication by \(c\).” Perhaps I should have assumed from the beginning that \(f\) is monic, since then \(c = 1\).]

(f) Using Maple, we compute the formal derivative of

\[
f = x^{11} - x^{10} + 2x^8 - 4x^7 + 3x^5 - 3x^4 + x^3 + 3x^2 - x - 1
\]

as follows:
> f := x^11-x^10+2*x^8-4*x^7+3*x^5-3*x^4+x^3+3*x^2-x-1;

\[
\begin{align*}
& x^{11} - x^{10} + 2x^8 - 4x^7 + 3x^5 - 3x^4 + x^3 + 3x^2 - x - 1 \\
& \text{\texttt{\textcolor{red}{fprime := diff(f, x)}};}
\end{align*}
\]

Now we compute \( f_{\text{red}} \) using the formula in (e):

```text
> quo(f, gcd(f, fprime), x);

\[
\begin{align*}
& x^5 + x^2 - x - 1 \\
& \text{\texttt{\textcolor{red}{\textit{Hence by (c):}}}}
\end{align*}
\]
```

\[
I(V(x^{11}-x^{10}+2x^8-4x^7+3x^5-3x^4+x^3+3x^2-x-1)) = (x^5+x^2-x-1).
\]