CS711 Assignment 1

Sankalp Gambhir
180260032

August 19, 2021

Question 1.

Proof. Given, $\mathbb{F}$ is a field of characteristic p, assumed prime. Then, over the polynomial ring $\mathbb{F}[x, y]$, we evaluate the expression $(x + y)^p$.

Since field multiplication is commutative, we may write the binomial expansion of the expression, with coefficients c_i yet undetermined as

$$(x+y)^p = \sum_{i=0}^{p} c_i \cdot x^i y^{p-i} \quad . \tag{1}$$

It is easy to see that $c_i = \sum_{j=1}^{\binom{p}{i}} 1$, $1 \in \mathbb{F}$, i.e., $\binom{p}{i} \in \mathbb{Z}$ terms of the form $x^i y^{p-i}$ were obtained and summed. Clearly, $c_0 = c_p = 1$, and $\forall i \in \mathbb{N}$, and $i < p$, we have

$$\binom{p}{i} = \frac{p!}{(p-i)! \cdot i!} = \frac{p \cdot (p-1)!}{(p-i)! \cdot i!} \quad . \tag{2}$$

In the factorial, and subsequently prime expansion of the denominator, every number obtained will be smaller than p, and by virtue of p being prime, will not divide the term in the numerator, leading to $\binom{p}{i}$ being divisible by p. And due to p being the characteristic of the field $\mathbb{F}$, we have

$$\forall i \; \exists k_i \; \binom{p}{i} = p \cdot k_i, \text{ and} \tag{3}$$

$$c_i = \sum_{j=1}^{k_i} \left(\sum_{n=1}^{p} 1 \right) = \sum_{j=1}^{k_i} 0 = 0 \; . \tag{4}$$

Thus, we have $(x + y)^p = x^p + y^p$.

□

Question 2.

(a) *Proof.* We prove the full-rank property of the Vandermonde matrix (denoted here as V_n) as defined via induction.

Base case: $n = 1$. We have

$$V_1 = \begin{bmatrix} 1 \end{bmatrix} \tag{5}$$

is clearly of full rank. The base case is clear.

Induction: Suppose $\forall m \in \mathbb{N}$ with $m < n$ implies V_m is of full rank. Then consider the matrix V_n over $\{\alpha_i\}$ then for V_n to be of full rank, the vectors $\vec{A_i} = (\alpha_i^j)$ must form a set of n linearly independent vectors. If possible, consider that the $\{A_i\}$ to be linearly dependent instead. Then, there exist scalars $\{c_i\}$ such that

$$\sum_{i=1}^{n} c_i \vec{A_i} = 0 \text{ , or} \tag{6}$$

$$\forall i \sum_{j=0}^{n-1} c_j \cdot \alpha_i^j = 0 \text{ .} \tag{7}$$

Consider the polynomial formed with these (c_i) as coefficients, $f(x) = \sum_{j=0}^{n-1} c_j \cdot x^j$, with Degree$(f) = (n-1)$. We know of n roots of this polynomial from Equation 7, of the set $\{\alpha_i\}$. However, this clearly violates the fact the that the number of roots must be less than or equal to the degree of the polynomial. Thus, we have a contradiction, and V_n is indeed of full rank. □

(b) *Proof.* Consider the determinant of V_n as defined above instead as a function over one of the α_i, replacing it with a variable x in the field. As we choose $x = \alpha_j$ for $j < i$, we find that the determinant vanishes due to having two identical rows. The determinant being a polynomial (of degree $(n-1)$ in x), must have $(x - \alpha_j)$ as divisors. Repeating this for each i, we find that the determinant must be divisible by the product polynomial $\prod_{j<i}(\alpha_i - \alpha_j)$, i.e.

$$\exists q(x) \in \mathbb{F}[x] \; |V_n| = q(\{\alpha_k\}) \cdot \prod_{j<i} (\alpha_i - \alpha_j) \text{ .} \tag{8}$$

The product contains each α_i exactly $(n-1)$ times, which can also by a first step expansion be verified to be the degree of the determinant in α_i. So, $q(\alpha_k)$ may not contain any terms involving α_i. Likewise it follows for all other parameters. Hence, $q(\{\alpha_k\})$ is a scalar, which by painstaking inductive expansion can be verified to be 1 as well. □

Question 3.

Proof. First, I argue by explicit construction that a polynomial as required exists, followed by a proof for the uniqueness of this construction.

Construct, for each pair (α_i, β_i), a polynomial $f_i(x)$ such that $f_i(\alpha_j) = \delta_{ij} \cdot \beta_i \forall$ index pairs (i, j). A choice for such a polynomial is:

$$f_i(x) = \beta_i \cdot \frac{\prod_{j \neq i}(x - \alpha_j)}{\prod_{j \neq i}(\alpha_i - \alpha_j)} \tag{9}$$

which is a polynomial of degree $(n-1)$ satisfying the required criteria. The sum of all such polynomials produces the required result:

$$f(x) = \sum_{i=1}^{n} f_i(x) \ . \tag{10}$$

The existence of the required polynomial is proven. Assume now there are two distinct polynomials $f(x)$ and $g(x)$, each with degree less than $(n-1)$, satisfying the requirements. Thus, they each have monomial expansions of the form

$$f(x) = \sum_{j=0}^{n-1} a_j x^j \ \text{, and} \tag{11}$$

$$g(x) = \sum_{j=0}^{n-1} b_j x^j \ . \tag{12}$$

For each of these, plugging in the values of the given points, we get the linear systems

$$\begin{aligned}
\sum_{j=0}^{n-1} a_j \alpha_1^j &= \beta_1 \\
\sum_{j=0}^{n-1} a_j \alpha_2^j &= \beta_2 \\
&\vdots \\
\sum_{j=0}^{n-1} a_j \alpha_n^j &= \beta_n
\end{aligned}$$

and likewise for $g(x)$, with the b_j as coefficients. This can be seen as a linear system given by the Vandermonde matrix and the vector (β_j), with the vectors (a_j) and (b_j) as solutions to the system. However, from the previous question we know that the Vandermonde matrix is in fact of full rank, so there is a unique solution to this linear system, and thus the solution vectors must be equal, i.e., $a_j = b_j \forall j \in \{1, 2, ..., n\}$. Consequently, $f(x) = g(x)$, so we have a contradiction. There is thus a unique polynomial satisfying the given requirements. □

Question 4.

(a) *Proof.* Forward ($\Rightarrow$) direction:
α is zero of multiplicity atleast k. Then $\forall i \in \mathbb{N}$, with $i \leq k$, we have

$$\frac{\partial^i f}{\partial x^i}(\alpha) = 0. \tag{13}$$

In particular, for $i = 0$ we find that α is a root of the polynomial. And thus we can write $f(x) = (x-\alpha)q_0(x)$ for some polynomial $q_0(x)$ of degree one less than $f(x)$. Differentiating this expression, we obtain the polynomial $f'(x) = q_0(x) + (x-\alpha)q_0'(x)$, which due to Equation 13, also has α as a root, and we find that in fact, $q_0(x) = (x-\alpha)q_1(x)$ for a polynomial $q_1(x)$ as before. Continuing this up to k differentiations we find $\exists q_k(x) \in \mathbb{C}[x]$, such that $f(x) = (x-\alpha)^k \cdot q_k(x)$ as required per the definition of divisibility.

Backward ($\Leftarrow$) direction:
Given, $\exists \alpha, k$ such that $(x-\alpha)^k$ divides the polynomial $f(x)$, i.e. we can write for some $q(x) \in \mathbb{C}[x]$, $f(x) = (x-\alpha)^k \cdot q(x)$.

Define the set $D_n \subseteq \mathbb{C}[x]$ for each n containing all the polynomials from the ring which are divisible by $(x-\alpha)^n$. This is a descending chain of ideals. We note two things, first, $\forall n, D_n \subseteq D_{n-1}$, and second, $f(x) \in D_k$. I induct over n to show the desired property:

$$\forall t(x) \in D_n, \frac{\partial^n t}{\partial x^n}(\alpha) = 0 \ . \tag{14}$$

Also note, two corollaries of the definition, $\forall t(x) \in D_n$, we have:

1. $t'(x) \in D_{n-1}$, and
2. $(x-\alpha) \cdot t(x) \in D_{n+1}$.

Base case:

$\forall t(x) \in D_0$, since $t(\alpha) = 0$, then we have $\frac{\partial^0 t}{\partial x^0}(\alpha) = t(\alpha) = 0$. So, the base case is clear.

Induction:

Given that $\forall m \in \mathbb{N}$ with $m < n, D_m$ satisfies the property in Equation 14, we write for some $t(x) \in D_n$,

$$\exists q_t(x) \in D_{n-1} \text{ such that } t(x) = (x-\alpha)q_t(x), \tag{15}$$

$$\frac{\partial t}{\partial x}(x) = (x-\alpha)q_t'(x) + q_t(x), \text{ and} \tag{16}$$

$$\frac{\partial^n t}{\partial x^n}(x) = \frac{\partial^{n-1}}{\partial x^{n-1}}(x-\alpha)q_t'(x) + \frac{\partial^{n-1}}{\partial x^{n-1}}q_t(x)\ . \tag{17}$$

Using the corollaries noted above, we see that the operands of the differential operators on the right in the last equation are both in D_{n-1}, and thus the right side evaluates to zero on substituting $x = \alpha$. So,

$$\frac{\partial^n t}{\partial x^n}(\alpha) = 0\ , \tag{18}$$

and the induction is complete.

Since $f(x) \in D_k$, it satisfies the required property.

□

(b) *Proof.* Due to the algebraic completeness of the complex field, and the Fundamental Theorem of Algebra, we can write:

$$f(x) = c \cdot \prod_i (x-\beta_i)^{k_i}\ , \tag{19}$$

where the $\{(\beta_i, k_i)\}$ are the roots of the polynomial and their degrees respectively, and c is a complex scalar. It is easy to see from part (a) and this equation that in fact $\text{Mult}(f, \beta_i) = k_i \forall i$ and by expanding the polynomial we note $\sum_i k_i = \text{Degree}(f)$.

We can thus write

$$\sum_i \text{Mult}(f, \beta_i) = \text{Degree}(f)\ , \text{ and} \tag{20}$$

$$\text{Mult}(f, \alpha) = 0 \text{ if } \nexists i\ \alpha = \beta_i\ . \tag{21}$$

Now, for an arbitrary set $S = \{\alpha_1, \alpha_2, ..., \alpha_n\} \subseteq \mathbb{C}$, we write the sum of multiplicities due to Equation 21 as

$$\sum_{\alpha \in S} \text{Mult}(f, \alpha) = \sum_{\alpha \in S \cap \{\beta_i\}} \text{Mult}(f, \alpha)\ . \tag{22}$$

where the right side is identified easily as a subset of the sum in Equation 20, and thus we obtain

$$\sum_{\alpha \in S} \text{Mult}(f, \alpha) \leq \text{Degree}(f)\ . \tag{23}$$

□