Soham Chatterjee
Email: soham.chatterjee@tifr.res.in
Course: Algebra, Number Theory and Computation

Assignment - 1
Dept: STCS, TIFR
Date: March 4, 2025

Problem 1 5 Points

Let $\mathbb{F}$ be a field of characteristic equal to p. Then, show that over the polynomial ring $\mathbb{F}[x,y]$, $(x+y)^p = x^p + y^p$

Solution:

Lemma 1. $p \mid \binom{p}{k} \iff 0<k<p$

Proof: Let $0<k<p$. Then $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. As $0<k<p$, $0<p-k<p$. Since p is a prime none of numbers from 0 to $\max\{k,p-k\}$ divides p. Therefore p never gets canceled out in $\binom{p}{k}$. Hence $p \mid \binom{p}{k}$.

Now suppose $p \mid \binom{p}{k}$. Now

$$\binom{p}{k} = \frac{p!}{k!}(p-k)! = \frac{\prod_{i=1}^{k}(p-k+i)}{k!} = \frac{\prod_{i=1}^{p-k}(k+i)}{(p-k)!}$$

Now the highest power of p that divides $\prod_{i=1}^{k}(p-k+i)$ and $\prod_{i=1}^{p-k}(k+i)$ is 1. Therefore $p \nmid k!$ and $p \nmid (p-k)!$. Therefore $k<p$ and $p-k<p$. Hence we have $0<k<p$. □

So now using the lemma we have $(x+y)^p = x^p+y^p+\sum_{i=1}^{p-1}\binom{p}{i}x^{p-i}y^i = x^p+y^p+p\cdot C$ where $p\cdot C = \sum_{i=1}^{p-1}\binom{p}{i}x^{p-i}y^i$. Since the characteristic of the field is p we have $p\cdot C = 0$. Hence $(x+y)^p = x^p+y^p$. ■

Problem 2 20 Points

Let q be a prime power and let $k>0$ be a natural number. The polynomial $\mathsf{Trace}(x)$ is defined as

$$\mathsf{Trace}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{k-1}}$$

(a) **(5 points)** Show that for every $\alpha \in \mathbb{F}_{q^k}$, $\mathsf{Trace}(\alpha) \in \mathbb{F}_q$.

(b) **(5 points)** Show that when viewed as a map from the vector space $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$. Trace is $\mathbb{F}_q$-linear.

(c) **(10 points)** Using the properties of Trace, conclude that for *every* $\mathbb{F}_q$ linear map L from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$, there is an $\alpha_L \in \mathbb{F}_{q^k}$ such that for all $\beta \in \mathbb{F}_{q^k}$, $L(\beta) = \mathsf{Trace}(\alpha_L\cdot\beta)$.

Solution:

(a) The Frobenius map $\varphi: \mathbb{F}_{q^k} \longrightarrow \mathbb{F}_{q^k}$, where $\varphi(x) = x^q$ is an automorphism and it is $\mathbb{F}_q$-linear and the only elements for which $\varphi(x) = x$ are the elements of $\mathbb{F}_q$.

Lemma 2. *The maps Trace and φ commutes over $\mathbb{F}_{q^k}$.*

Proof:

$$\begin{aligned}\mathsf{Trace}\circ\varphi(x) = \mathsf{Trace}(x^q) &= x^q + (x^q)^q + (x^q)^{q^2} + \cdots + (x^q)^{q^{k-1}} \\ &= x^q + \left(x^{q^2}\right)^q + \left(x^{q^3}\right)^q + \cdots + \left(x^{q^{k-1}}\right)^q \\ &= \left(x + x^q + x^{q^2} + \cdots + x^{q^{k-1}}\right)^q = (\mathsf{Trace}(x))^q = \varphi\circ\mathsf{Trace}(x)\end{aligned}$$

Hence two maps commutes. $\square$

Now notice that for any $\alpha \in \mathbb{F}_{q^k}$

$$\mathsf{Trace}(\alpha)^q = \mathsf{Trace}(\alpha^q) = \sum_{i=0}^{k-1} (\alpha^q)^{q^i} = \sum_{i=0}^{k-1} \alpha^{q^{i+1}} = \sum_{i=1}^{k} \alpha^{q^i} = \sum_{i=0}^{k-1} \alpha^{q^i} = \mathsf{Trace}(\alpha)$$

The third from the last inequality is true is because $\alpha^{q^k} = \alpha$ for all $\alpha \in \mathbb{F}_{q^k}$. Hence for all $\alpha \in \mathsf{Range}(\mathsf{Trace})$. $\varphi(\alpha) = \alpha$. Now the only elements which remains same under the Frobenius map are the elements of $\mathbb{F}_q$. Therefore $\mathsf{Range}(\mathsf{Trace}) \subseteq \mathbb{F}_q$. So the for all $\alpha \in \mathbb{F}_{q^k}$, $\mathsf{Trace}(\alpha) \in \mathbb{F}$.

(b) Suppose $a, b \in \mathbb{F}_{q^k}$ and $\alpha \in \mathbb{F}_q$. Then we have

$$\begin{aligned}\mathsf{Trace}(\alpha \cdot a + b) = \sum_{i=0}^{k-1} (\alpha \cdot a + b)^{q^i} = \sum_{i=0}^{k-1} (\alpha \cdot a)^{q^i} + b^{q^i} &= \sum_{i=0}^{k-1} \left(\alpha \cdot a^{q^i} + b^{q^i}\right) \\ &= \alpha \left(\sum_{i=0}^{k-1} a^{q_i}\right) + \left(\sum_{i=0}^{k-1} b^{q_i}\right) = \alpha\,\mathsf{Trace}(a) + \mathsf{Trace}(b)\end{aligned}$$

Therefore $\mathsf{Trace}(x)$ is a $\mathbb{F}_q$-linear map.

(c) Let $S = \{L : \mathbb{F}_{q^k} \to \mathbb{F}_q \mid L \text{ is } \mathbb{F}_q - \text{linear}\}$. As $\mathbb{F}_{q^k}$ forms a vector space over $\mathbb{F}_q$ the set S also forms a vector space over $\mathbb{F}_q$ and actually called the dual of $\mathbb{F}_q$. Since dimension of the vector space $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ is k we have the dimension of S over $\mathbb{F}_q$ is also k.

Now since dimension of $\mathbb{F}_{q^k}$ is k over $\mathbb{F}_q$ there exists k elements of $\mathbb{F}_{q^k}$, $\{\beta_1, \dots, \beta_k\} \subseteq \mathbb{F}_{q^k}$ such that they form a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Then consider the collection of maps $\{\mathsf{Trace}(\beta_i \cdot x) \mid i \in [k]\}$. We will show that these maps are linearly independent. And since they are $\mathbb{F}_q$-linear they are in S. Since they form a k size collection of linearly independent $\mathbb{F}_q$-linear maps they span the set S.

Lemma 3. *$\{\mathsf{Trace}(\beta_i \cdot x) \mid i \in [k]\}$ are linearly independent.*

Proof: Suppose they are linearly dependent. Let there exists $\gamma_i \in \mathbb{F}_q$ for all $i \in [k]$ not all zero such that $\sum_{i=1}^{k} \gamma_i \,\mathsf{Trace}(\beta_i \cdot x) \equiv 0$. Then we have

$$\sum_{i=1}^{k} \gamma_i \,\mathsf{Trace}(\beta_i \cdot x) = \sum_{i=1}^{k} \mathsf{Trace}((\gamma_i \beta_i) \cdot x) = \mathsf{Trace}\left(\left(\sum_{i=1}^{k} \gamma_i \beta_i\right) x\right)$$

Therefore $\mathsf{Trace}\left(\left(\sum_{i=1}^{k} \gamma_i \beta_i\right) \alpha\right) = 0$ for all $\alpha \in \mathbb{F}_{q^k}$. Since $\beta_i's$ are linearly independent $\sum_{i=1}^{k} \gamma_i \beta_i \neq 0$. Let $\delta := \sum_{i=1}^{k} \gamma_i \beta_i$. Then $\mathsf{Trace}(\delta \cdot \alpha) = 0$ for all $\alpha \in \mathbb{F}_{q^k}$. But that means every element of $\mathbb{F}_{q^k}$ is a root of $\mathsf{Trace}(x)$ but that is not possible since $\deg \mathsf{Trace}(x) = q^{k-1}$. Hence contradiction. Therefore $\{\mathsf{Trace}(\beta_i \cdot x) \mid i \in [k]\}$ are linearly independent. $\square$

Therefore the set $\{\mathsf{Trace}(\beta_i \cdot x) \mid i \in [k]\}$ spans the set of $\mathbb{F}_q$-linear maps over $\mathbb{F}_{q^k}$. Now let $L \in S$. Then there exists $\gamma_i \in \mathbb{F}$ for all $i \in [k]$ such that $L = \sum_{i=1}^{k} \gamma_i \,\mathsf{Trace}(\beta_i \cdot x) = \sum_{i=1}^{k} \mathsf{Trace}(\gamma_i \beta_i \cdot x) = \mathsf{Trace}\left(\left(\sum_{i=1}^{k} \gamma_i \beta_i\right) x\right) = L(\alpha_L \cdot x)$ where $\alpha_L = \sum_{i=1}^{k} \gamma_i \beta_i$.

$\blacksquare$

Problem 3 10 Points

Let q be a prime power, $k > 0$ be a natural number and let $S \subset \mathbb{F}_{q^k}$ be a subspace of $\mathbb{F}_{q^k}$ of dimension s, when we view $\mathbb{F}_{q^k}$ as a k dimensional linear space over $\mathbb{F}_q$. Consider the polynomial $P_S(x)$ defined as

$$P_S(x) = \prod_{\alpha \in S} (x - \alpha)$$

Show that there exist $\beta_1, \beta_2, \dots, \beta_s \in \mathbb{F}_{q^k}$ such that

$$P_S(x) = x_{q^s} + \beta_1 x^{q^{s-1}} + \beta_2 x^{q^{s-2}} + \cdots + \beta_s x$$

Solution: The dimension of S over $\mathbb{F}_q$ in $\mathbb{F}_{q^k}$ is s. Therefore there exists $\gamma_1, \dots, \gamma_s$ which forms a basis of S over $\mathbb{F}_q$. Denote the followings:

$$M(x) := \begin{bmatrix} \gamma_1 & \gamma_1^q & \gamma_1^{q^2} & \cdots & \gamma_1^{q^s} \\ \gamma_2 & \gamma_2^q & \gamma_2^{q^2} & \cdots & \gamma_2^{q^s} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma_s & \gamma_s^q & \gamma_s^{q^2} & \cdots & \gamma_s^{q^s} \\ x & x^q & x^{q^2} & \cdots & x^{q^s} \end{bmatrix} \qquad \delta := \det \begin{pmatrix} \gamma_1 & \gamma_1^q & \gamma_1^{q^2} & \cdots & \gamma_1^{q^{s-1}} \\ \gamma_2 & \gamma_2^q & \gamma_2^{q^2} & \cdots & \gamma_2^{q^{s-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma_s & \gamma_s^q & \gamma_s^{q^2} & \cdots & \gamma_s^{q^{s-1}} \end{pmatrix}$$

Then consider the polynomial $f(x) = \det(M(x))$. Clearly we have

$$f(x) = \delta x^{q^s} + f_1 x^{q^{s-1}} + f_2 x^{q^{s-2}} + \cdots + f_s x$$

for some $f_i \in \mathbb{F}_{q^k}$ for all $i \in [s]$. Now if $\delta = 0$ then matrix $\begin{bmatrix} \gamma_1 & \gamma_1^q & \gamma_1^{q^2} & \cdots & \gamma_1^{q^{s-1}} \\ \gamma_2 & \gamma_2^q & \gamma_2^{q^2} & \cdots & \gamma_2^{q^{s-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma_s & \gamma_s^q & \gamma_s^{q^2} & \cdots & \gamma_s^{q^{s-1}} \end{bmatrix}$ is not full rank i.e. the rows of the matrix are not linearly independent. Hence γ_i's are not linearly independent which is not possible. Therefore $\delta \neq 0$. Hence the polynomial $f(x)$ has degree x^{q^s}. Now consider the modified polynomial $\tilde{f}(x) = x^{q^s} + \sum_{i=1}^{s} \tilde{f}_i x^{q^i}$ where $\tilde{f}_i = \frac{f_i}{\delta}$

Lemma 4. $\operatorname{rank}(M(\alpha)) < n \iff \alpha \in S$

Proof: Let $\alpha \in S$. Then there exists $c_i \in \mathbb{F}_q$ such that $\alpha = \sum_{i=1}^{k} c_i \beta_i$. Then $\alpha^{q^j} = \sum_{i=1}^{k} c_j \beta_i^{q^j}$ for all $j \in \mathbb{Z}_{\geq 0}$. There for the rows of $M(\alpha)$ are not linearly independent. Hence $\operatorname{rank}(M(x)) < n$.

Now suppose $\operatorname{rank}(M(\alpha)) < n$ for some $\alpha \in \mathbb{F}_{q^k}$. Then the rows of $M(\alpha)$ are not linearly independent. Hence there exists $c_i \in \mathbb{F}_q$ for all $i \in [k]$ such that $\sum_{i=1}^{k} c_i \gamma_i = \alpha$. Hence $\alpha \in S$. □

Hence with the lemma we get that

$$\det(M(\alpha)) = 0 \iff \operatorname{rank}(M(\alpha)) < n \iff \alpha \in S$$

Hence the roots of $\tilde{f}$ are all the elements of S.

Now both $\tilde{f}$ and P_S are nonzero, monic, has degree x^{q^s} and they have the same set of roots. Therefore $\tilde{f}(x) = P_S(x)$. Therefore we can express $P_S(x)$ as

$$P_S(x) = x^{q^s} + \tilde{f}_1 x^{q^{[s-1]}} + \tilde{f}_2 x^{q^{s-2}} + \cdots + \tilde{f}_s x$$

■

Problem 4 20 Points

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ distinct elements of some field $\mathbb{F}$. And, let $V(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be the $n \times n$ matrix whose (i, j) entry equals α_i^{j-1}.

(a) **(5 points)** Show that V has rank equal to n.

(b) **(10 points)** Show that the determinant of V equals $\prod_{i<j}(\alpha_j - \alpha_i)$

(c) **(5 points)** For every $\beta_1, \beta_2 \ldots, \beta_n \in \mathbb{F}$, show that there is a unique polynomial $f \in \mathbb{F}[x]$ of degree at most $n-1$ such that for every $i \in \{1, 2, \ldots, n\}$, $f(\alpha_i) = \beta_i$.

Solution:

(a) Suppose the rank of V is less than n. Then the columns of V are linearly dependent. Then there exists $\beta_j \in \mathbb{F}$ for all $j \in [n]$ not all zero such that for all $i \in [n]$ $\sum_{j=1}^{n} \beta_j \cdot \alpha_i^{j-1} = 0$. Then consider the polynomial $f \in \mathbb{F}[x]$ where $f(x) = \sum_{i=1}^{n} \beta_i x^{i-1}$. Then we conclude that $f(\alpha_i) = 0$ for all $i \in [n]$. Therefore roots of f are $\alpha_1, \alpha_2, \ldots, \alpha_n$. But $\deg f \leq n-1$. Hence f cannot have more than $n-1$ roots. Hence contradiction. Therefore rank of V is n.

(b) We will prove this using induction on n. For base case $n = 1$. $V(\alpha)$ contains only one element 1. Hence this is true. Suppose this is true for $n-1$. Now

$$\det\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \alpha_1^3 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \alpha_2^3 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 1 & \alpha_n & \alpha_n^2 & \alpha_n^3 & \cdots & \alpha_n^{n-1} \end{pmatrix} = \det\begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & \alpha_2 - \alpha_1 & \alpha_2^2 - \alpha_1\alpha_2 & \alpha_2^3 - \alpha_1\alpha_2^2 & \cdots & \alpha_2^{n-1} - \alpha_1\alpha_2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 1 & \alpha_n - \alpha_1 & \alpha_n^2 - \alpha_1\alpha_n & \alpha_n^3 - \alpha_1\alpha_n^2 & \cdots & \alpha_n^{n-1} - \alpha_1\alpha_n^{n-2} \end{pmatrix}$$

$$= \prod_{i=2}^{n}(\alpha_i - \alpha_1)\det\begin{pmatrix} 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-2} \end{pmatrix}$$

By inductive hypothesis we have

$$\det(V(\alpha_2, \ldots, \alpha_n)) = \det\begin{pmatrix} 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-2} \end{pmatrix} = \prod_{2 \leq i < j \leq n}(\alpha_j - \alpha_i)$$

Therefore

$$\det(V(\alpha_1, \ldots, \alpha_n)) = \prod_{1 \leq i < j \leq n}(\alpha_j - \alpha_i)$$

Therefore by mathematical induction this is true for all $n \in \mathbb{N}$.

(c) Consider the vector $\hat{f} = \begin{bmatrix} f_0 & f_1 & \cdots & f_{n-1} \end{bmatrix}^T$ where f_i's denote the coefficients of the polynomial $f(x) = \sum_{i=0}^{n} f_i x^i$ for which $f(\alpha_i) = \beta_i$ and the vector $b = \begin{bmatrix} \beta_1 & \beta_2 & \cdots & \beta_n \end{bmatrix}^T$. Now such a polynomial f exists if and only if the equation $V\hat{f} = b$ is satisfied. Since V has full rank V is invertible. Hence we get a $\hat{f} = V^{-1}b$. Therefore the equation has a unique solution. Hence there exists an unique polynomial f such that $f(\alpha_i) = \beta_i$.

∎

Problem 5 20 Points

Let $\mathbb{F}$ be any field. $\alpha \in \mathbb{F}$ is said to be a zero (or root) of multiplicity at least k of a non-zero polynomial $f(x) \in \mathbb{F}[x]$ if $f(\alpha) = \frac{\partial f}{\partial x}(\alpha) = \cdots = \frac{\partial^{k-1} f}{\partial x^{k-1}}(\alpha) = 0$ and $\frac{\partial^k f}{\partial x^k}(\alpha) \neq 0$.

(a) (**10 points**) Show that α is a zero of multiplicity at least k of f if and only if $(x-\alpha)^k$ divides $f(x)$.

(b) (**10 points**) If $\alpha_1, \alpha_2, \ldots, \alpha_t$ are distinct elements of $\mathbb{C}$, then show that

$$\sum_{i=1}^{t} (\mathrm{Mult}(f, \alpha_i)) \leq \mathrm{Degree}(f)$$

where $\mathrm{Mult}(f, \alpha_i)$ denotes the multiplicity of f at α_i.

Solution:

(a) We will denote $f^{(i)}(x) = \frac{\partial^i f}{\partial x^i}(x)$ where $f^{(0)}(x) = f(x)$.

$(\Leftarrow)$: We will prove this using induction on k¿ For base case $k = 1$. Then $(x - \alpha) \mid f(x)$. Hence α is a root of f. Therefore α is a zero of f with multiplicity at least 1. Suppose this is true for $k - 1$. Now we will show for k. Let $(x - \alpha)^k \mid f(x)$. Since α is a root of f we have $f(x) = (x - \alpha)g(x)$ for some $g(x) \in \mathbb{F}[x]$. Now $(x - \alpha)^{k-1} \mid g(x)$. Therefore by inductive hypothesis α is a zero of g with multiplicity at least $k - 1$ i.e. $g^{(i)}(\alpha) = 0$ for all $i \in \{0, \ldots, k - 2\}$ and since g is not a zero polynomial there exists $l > k - 2$ such that $g^{(l)}(\alpha) \neq 0$.

Lemma 5. $f^{(i)}(x) = ig^{(i-1)}(x) + (x - \alpha)g^{(i)}(x)$

Proof: We will prove this using induction on i. For base case $i = 1$. Then $f^{(1)}(x) = g(x) + (x - \alpha)g^{(1)}(x)$. So base case is true. Let this is true for $i - 1$. Now

$$f^{(i-1)} = (i-1)g^{(i-2)}(x) + (x-\alpha)g^{(i-1)}(x) \implies$$
$$f^{(i)}(x) = (i-1)g^{(i-1)}(x) + g^{(i-1)}(x) + (x-\alpha)g^{(i)} = ig^{(i-1)}(x) + (x-\alpha)g^{(i)}(x)$$

Hence by mathematical induction this is true. □

Therefore $f^{(i)}(\alpha) = ig^{(i-1)}(\alpha) = 0$ for all $i \in [k-1]$ and $f^{(l+1)}(\alpha) = (l+1)g^{(l)}(\alpha) \neq 0$ where $l > k - 2$. Therefore $f^{(i)}(\alpha) = 0$ for all $i \in \{0, \ldots, k-1\}$ and $f^{(l+1)}(\alpha) \neq 0$ where $l + 1 > k - 1$. Therefore α is a zero of f with multiplicity at least k.

$(\Rightarrow)$: We will do induction on k. For base case $k = 1$. Then $f(\alpha) = 0$ and $\frac{\partial f}{\partial x}(\alpha) \neq 0$. Therefore $(x - \alpha) \mid f$. Hence the base case follows. Now suppose this is true for $k - 1$.

We will prove for k. Now $f^{(i)}(\alpha) = 0$ for all $i \in \{0, \ldots, k-1\}$ and there exists $l > k - 1$ such that $f^{(l)}(\alpha) \neq 0$. Therefore $f(x) = (x-\alpha)g(x)$ for some $g \in \mathbb{F}[x]$. Then $f^{(i)}(x) = ig^{(i-1)}(x) + (x-\alpha)g^{(i)}(x)$. Now consider the polynomial $g(x)$. We have $g^{(i)}(\alpha) = 0$ for all $i \in \{0, \ldots, k-2\}$ and $g^{(l-1)}(\alpha) \neq 0$. Hence α is a zero of g with multiplicity at least $k-1$. Therefore by inductive hypothesis we have $(x-\alpha)^{k-1} \mid g(x)$. Hence $(x-\alpha)^k \mid f(x)$. Therefore by mathematical induction this is true.

(b) Since f is over $\mathbb{C}$, f completely splits over $\mathbb{C}$. Now for any $\alpha \in \mathbb{C}$ we have by the above part that $(x - \alpha)^{\mathrm{Mult}(f,\alpha)} \mid f(x)$.

We will prove this by induction on n. For base case $n = 1$ then for α_1 we have

$$(x-\alpha_1)^{\mathrm{Mult}(f,\alpha_1)} \mid f(x) \implies (x-\alpha_1)^{\mathrm{Mult}(f,\alpha_1)} g_1(x) = f(x) \implies \mathrm{Mult}(f, \alpha_1) \leq \mathrm{Degree}(f)$$

So base case follows. Suppose this is true for $n-1$. We will prove for n now. Now if $\mathrm{Mult}(f,\alpha_i)=0$ for any $i\in[n]$ then

$$\sum_{j=1}^{n}\mathrm{Mult}(f,\alpha_j)=\sum_{j=1,j\neq i}^{n}\mathrm{Mult}(f,\alpha_i)$$

Therefore by inductive hypothesis this is true. So assume $\mathrm{Mult}(f,\alpha_i)>0$ for all $i\in[n]$. Then $f(x)=(x-\alpha_1)^{\mathrm{Mult}(f,\alpha_1)}g(x)$ for some $g\in\mathbb{C}[x]$. Hence $\deg(f)=\mathrm{Mult}(f,\alpha_1)+\deg(g)$. Now $(x-\alpha_i)$'s are relatively coprime with each other. Therefore $(x-\alpha_i)^{\mathrm{Mult}(f,\alpha_i)}$'s are also relatively coprime with each other. Hence $(x-\alpha_i)^{\mathrm{Mult}(f,\alpha_i)}\mid g(x)$ for all $i\in\{2,\ldots,n\}$. Now by inductive hypothesis we have $\sum\limits_{i=2}^{n}\mathrm{Mult}(f,\alpha_i)\leq\mathrm{Degree}(g)$. Therefore we have $\sum\limits_{i=1}^{n}\mathrm{Mult}(f,\alpha_i)\leq\mathrm{Degree}(f)$. Hence this is true for all n.

∎