**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 $0 < k < p$. $\qquad\square$

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 $(x + y)^p = x^p + y^p$. $\qquad\blacksquare$

---

**Problem 2**                                                                                    20 Points

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

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

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

(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 $\beta \in \mathbb{F}_{q^k}$, $L(\beta) = \text{Trace}(\alpha_L \cdot \beta)$.

**Solution:**

(a) The Frobenius map $\varphi : \mathbb{F}_{q^k} \to \mathbb{F}_{q^k}$, 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 $\varphi$ commutes over $\mathbb{F}_{q^k}$.*

**Proof:**

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

$$= x^q + \left(x^{q^2}\right)^q + \left(x^{q^3}\right)^q + \cdots + \left(x^{q^{k-1}}\right)^q$$

$$= \left(x + x^q + x^{q^2} + \cdots + x^{q^{k-1}}\right)^q = (\text{Trace}(x))^q = \varphi \circ \text{Trace}(x)$$

Hence two maps commutes. □

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

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

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 $\alpha \in \text{Range(Trace)}$. $\varphi(\alpha) = \alpha$. Now the only elements which remains same under the Frobenius map are the elements of $\mathbb{F}_q$. Therefore $\text{Range(Trace)} \subseteq \mathbb{F}_q$. So the for all $\alpha \in \mathbb{F}_{q^k}$, $\text{Trace}(\alpha) \in \mathbb{F}$.

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

$$\text{Trace}(\alpha \cdot a + b) = \sum_{i=0}^{k-1} (\alpha \cdot a + b)^{q^i} = \sum_{i=0}^{k-1} (\alpha \cdot a)^{q^i} + b^{q^i} = \sum_{i=0}^{k-1} \left( \alpha \cdot a^{q^i} + b^{q^i} \right)$$

$$= \alpha \left( \sum_{i=0}^{k-1} a^{q_i} \right) + \left( \sum_{i=0}^{k-1} b^{q_i} \right) = \alpha \, \text{Trace}(a) + \text{Trace}(b)$$

Therefore $\text{Trace}(x)$ 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 $\mathbb{F}_{q^k}$, $\{\beta_1, \ldots, \beta_k\} \subseteq \mathbb{F}_{q^k}$ such that they form a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Then consider the collection of maps $\{\text{Trace}(\beta_i \cdot x) \mid i \in [k]\}$. 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.** $\{Trace(\beta_i \cdot x) \mid i \in [k]\}$ *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 $\sum_{i=1}^{k} \gamma_i \text{Trace}(\beta_i \cdot x) \equiv 0$. Then we have

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

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

Therefore the set $\{\text{Trace}(\beta_i \cdot x) \mid i \in [k]\}$ 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 $L = \sum_{i=1}^{k} \gamma_i \text{Trace}(\beta_i \cdot x) = \sum_{i=1}^{k} \text{Trace}(\gamma_i \beta_i \cdot x) = \text{Trace}\left( \left( \sum_{i=1}^{k} \gamma_i \beta_i \right) x \right) =$

$L(\alpha_L \cdot x)$ where $\alpha_L = \sum_{i=1}^{k} \gamma_i \beta_i$.

■

## 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 $\beta_1, \beta_2, \ldots, \beta_s \in \mathbb{F}_{q^k}$ 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:**

∎

## 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 $\alpha_i^{j-1}$.

(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)

(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 $\alpha$ 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

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

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

**Solution:**

(a)

∎