Question 1. *Prove that the set of all the non-zero elements in a field is a multiplicative group. Use Lagrange's Theorem to prove that in a finite field of m elements $x^m = x$ for every x.*

Solution. Let $\mathbb{F}$ be a field and $\mathbb{F}^*$ denote the set of all non-zero elements of $\mathbb{F}$. Prove that $\mathbb{F}$ is a multiplicative group. Since 1 is assumed to be distinct from 0, then $1 \in \mathbb{F}^*$ and it is the identity of $\mathbb{F}^*$, because

$$1 \cdot a = a \cdot 1 = a$$

for any $a \in \mathbb{F}$. Furthermore, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$ since otherwise we could multiply ab on b^{-1} (it exists, because $b \neq 0$) and get $a = 0$, which is not true. So, $\mathbb{F}$ is closed under multiplication. Finally, by one of the field axioms, any non-zero a has the multiplicative inverse, i. e. an element a^{-1}, satisfying

$$aa^{-1} = a^{-1}a = 1.$$

This means that $\mathbb{F}$ is closed under taking multiplicative inverses. Thus, $\mathbb{F}$ is a (commutative) group under multiplication.

If $\mathbb{F}$ consists of m elements, then $\mathbb{F}^*$ has the order $m - 1$, because $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$. By Lagrange theorem, the order of any element $a \in \mathbb{F}^*$ divides the order of $\mathbb{F}^*$, which is $m-1$. Therefore, $a^{m-1} = 1$ for any $a \in \mathbb{F}^*$. Multiplying both sides by a, we obtain $a^m = a$ for all $a \in \mathbb{F}^*$. But this is also true for $a = 0$, so $a^m = a$ for any $a \in \mathbb{F}$. $\square$