Abstract Algebra in Theoretical Computer Science

Example for the formality level required from a solution

Lecturer: Gil Cohen

Problem 7

Let $\mathbb{F}_{125}$ be the field of 125 elements. Consider the function $f\colon \mathbb{F}_{125} \to \mathbb{F}_{125}$ that is given by $f(x) = x^{31}$. What is the image of f? Prove your answer.

Solution

The image of f is $\mathbb{F}_5$. To see this, fix $x \in \mathbb{F}_{125}$. Observe that $f(x) = x^{1+5+25}$. Thus, $f(x)^5 = x^{5+25+125}$. As $x^{125} = x$ (on the account of $x \in \mathbb{F}_{125}$) it holds that $f(x)^5 = x^{1+5+25} = f(x)$. That is, $f(x)$ is a root of the polynomial $y^5 - y \in \mathbb{F}_5[y]$. Therefore, $f(x) \in \mathbb{F}_5$ and so the image of f is contained in $\mathbb{F}_5$.

To be prove the reverse inclusion, observe that for $0 \neq x \in \mathbb{F}_5$, $f(x) = x^{31} = x^{32}x^{-1}$. Now, $x^{32} = (x^4)^8 = 1^8 = 1$ and so $f(x) = x^{-1}$ for such x. As every nonzero element in $\mathbb{F}_5$ is an inverse of some element in $\mathbb{F}_5$ ($\mathbb{F}_5$ being a field), and since $f(0) = 0$, we conclude that the image of f is precisely $\mathbb{F}_5$.

Alternative solution (sktech)

We sketch another proof. For a nonzero $x \in \mathbb{F}_{125}$ it holds that $x^{124} = 1$. But $124 = 4 \cdot 31$ and so $f(x)^4 = 1$. This, together with the fact that $f(0) = 0$ yields that $f(x) \in \mathbb{F}_5$.

To prove the reverse inclusion, observe that $x^{31} = x \cdot (x^5)^6$. For $x \in \mathbb{F}_5$ this equals to $x \cdot x^6 = x^2 \cdot x^5 = x^3$. It is easy to check (a verification that needs to be included in the solution) that the function $g\colon \mathbb{F}_5 \to \mathbb{F}_5$ that is given by $g(x) = x^3$ is surjective, which concludes the proof.