Maiko Johannes Nicolaas Bergman, 1259946
Dustin Wilhelmus Maria Bessems, 1228685
Sander Leon Maria Cauberg, 1008909
Guy Jozef Corien Puts, 1232041
Rick Stolk, 1263722

September 23, 2018

2WF90 - Algebra for Security, Chapter 2.4 Exercise 12

12. Consider the element $a = X + (X^3 + X + 1)\mathbb{Q}[X]$ in $\mathbb{Q}[X]/(X^3 + X + 1)$.

(a) We show that $X^3 + X + 1$ is irreducible in $\mathbb{Q}[X]$ and conclude that $\mathbb{Q}[X]/(X^3 + X + 1)$:
Let $m, n \in \mathbb{Z}$ be relatively prime, and let $f(X) = aX^3 + bX^2 + cX + d \in \mathbb{Q}[X]$ be a polynomial with $a, b, c, d \in \mathbb{Z}$.
We prove that if m/n is a root of $f(X)$, then $m|d$ and $n|a$:
We assume that $\frac{m}{n}$ is a root of $f(X)$. $\frac{m}{n}$ is a root of $f(X)$, so $f(\frac{m}{n}) = 0$.
{Proof}
So, we have proved that if m/n is a root of $f(X)$, then $m|d$ and $n|a$.
{Proof}
So, we have proved that $f(X) = aX^3 + bX^2 + cX + d \in \mathbb{Q}[X]$ is irreducible. This applies for any $a, b, c,$ and$d \in \mathbb{Z}$. If we fill in the formula with $a = 1, b = 0, c = 1, d = 1$, we get the polynomial $X^3 + X + 1$.
So, we have proved that the polynomial $X^3 + X + 1$ is irreducible in $\mathbb{Q}[X]$. We show that $\mathbb{Q}[X]/(X^3+X+1)$ is a field: We have previously proved that the polynomial $X^3 + X + 1$ is irreducible in $\mathbb{Q}[X]$. A theorem provided during the lectures states that: $\mathbb{K}[X]/f$ is a field if and only if f is irreducible. If f is our irreducible polynomial $X^3 + X + 1$, and $\mathbb{K} = \mathbb{Q}$, we can say that, by the given theorem, $\mathbb{Q}[X]/(X^3 + X + 1)$ is a field.
QED