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 $\mathbb{Q}[X]$.
    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 conclude that $\mathbb{Q}[X]/(X^3 + X + 1)$ is a field.
    We prove that if m/n is a root of $f(X)$, then $m|d$ and $n|a$.