

Q2a: Since $\mathbb{F}_p(x)/s(x)\mathbb{F}_p(x)$ is a ring, to show that it is a field it suffices to show that it contains multiplicative inverses for nonzero elements. Let $[a(x)]_{s(x)} \in \mathbb{F}_p(x)/s(x)\mathbb{F}_p(x)$ be nonzero. Let $d(x) = \gcd(a(x), s(x))$. By A4Q3d, we have that $d(x)|s(x)$. Therefore, either $d(x) = c \cdot s(x)$ or $d(x) = c$. Note that we can not have $d(x) = c \cdot s(x)$ since we would have that $c \cdot s(x)|a(x)$ and so $[a(x)]_{s(x)} \equiv 0$, which can not happen by assumption. Thus $d(x) = c$. Without loss of generality, we can assume that $d(x) = 1$. Thus for some $u(x), v(x)$ we can write $1 = u(x)a(x) + v(x)s(x)$. We get that $v(x)s(x) = 1 - u(x)a(x)$. Therefore, $s(x)|1 - u(x)a(x)$ and so $[1]_{s(x)} \equiv [u(x)]_{s(x)} \cdot [a(x)]_{s(x)}$. Take $[a(x)]_{s(x)}^{-1} = [u(x)]_{s(x)}$. Thus $\mathbb{F}_p(x)/s(x)\mathbb{F}_p(x)$ is a field.

Q2b: It is sufficient to show that $f(x)$ not prime if and only if there exists a c such that $f(c) = 0$. We proceed with the forward implication. Suppose that $f(x)$ is not prime. Then there exists some $q(x), p(x) \in \mathbb{F}_p[x]$ whose product is $f(x)$ and whose degrees are both strictly less than that of $f(x)$. Thus we will either have that the degrees of $p(x), q(x)$ are either both 1 or 1 and 2. WLOG assume that $\deg(p) = 1$. Thus $p(x) = x - c$ for some $c \in \mathbb{F}_p$. We can therefore write $f(x) = (x - c)q(x)$. We see that $f(c) = 0$. Now we prove the reverse implication. If there exists some c where $f(c) = 0$, then we can write $f(x) = (x - c)q(x)$ for some $q(x)$. Thus $f(x)$ has two divisors.

Q2c: Since $\deg(f) = 3$, we can verify if it is a prime polynomial using 2b by checking if it has any roots in \mathbb{F}_5 . Indeed, $s(1) \equiv 4, s(2) \equiv 2, s(3) \equiv 2, s(4) \equiv 4, s(0) \equiv 3$. This polynomial has no roots and therefore is prime. Therefore using the proof of 2a, and the euclidean algorithm for polynomials, we can find the inverse of $[x^3 + 3x + 2]_{s(x)}$ by finding polynomials $u(x), v(x)$ which satisfy $u(x)(x^3 + 3x + 2) + v(x)s(x) = 1$. We can take $u(x) = 3$ and $v(x) = 3x$. By the proof of 2a, $[3]_{s(x)}$ will be the desired inverse.

Q2d: We can verify easily that $t(x)$ has no roots in \mathbb{F}_5 . By 2b it must be a prime polynomial. From 2c, we see that the polynomial $v(x) = 2x$ will satisfy the proof 2a, and will be our desired inverse.