

Q3a: We will show that ev is a ring homomorphism in several steps. First we claim that it is a group homomorphism from additive group $(\mathbb{F}_p[x], +)$ to $(Fun(\mathbb{F}_p, \mathbb{F}_p), +)$. First, note that

$$ev([0(x)]_p)(c) = ev([0]_p)(c) = [0]_p(c) = \sum_{k=0}^n 0 \cdot c^k = [0]_p$$

Now we show that it preserves the structure of addition. Let $a(x), b(x) \in \mathbb{F}_p[x]$. We see that

$$ev(a(x) + b(x))(c) = ev(a + b)(c) = \sum_{k=0}^n (a_k + b_k)c^k = \sum_{k=0}^n a_k c^k + \sum_{k=0}^n b_k c^k = ev(a(x))(c) + ev(b(x))(c)$$

We now show that it sends the multiplicative identity to the multiplicative identity.

$$ev(1(x))(c) = ev(1)(c) = \sum_{k=0}^n 1 \cdot c^0 = [1]_p$$

Finally it remains to show it preserves the structure of multiplication. Let $a(x), b(x) \in \mathbb{F}_p[x]$

$$ev(a(x) \cdot b(x))(c) = ev(a \cdot b)(c) = (a \cdot b)(c) = a(c) \cdot b(c) = ev(a(x))(c) \cdot ev(b(x))(c)$$

Therefore, ev is a ring homomorphism.

Q3b: Let $q(x) = x^p - x$. To show \tilde{ev} is well defined it must be shown that if $[f(x)]_{q(x)} = [g(x)]_{q(x)}$, then $\tilde{ev}([f(x)]_{q(x)}) = \tilde{ev}([g(x)]_{q(x)})$. Suppose that $[f(x)]_{q(x)} = [g(x)]_{q(x)}$. Then by the euclidian algorithm for polynomials, there exists $p_1(x), p_2(x), r(x)$ such that $f(x) = p_1(x)q(x) + r(x)$ and $g(x) = p_2(x)q(x) + r(x)$. Therefore,

$$\tilde{ev}([f(x)]_{q(x)})(c) = ev(r(x))(c) = \tilde{ev}([g(x)]_{q(x)})(c)$$

Hence this map is well defined. Note that it is also a ring homomorphism by almost the exact same reasoning as in 3a, since it is a field as well.

Q3c: Let $x^p - x = q(x)$. Suppose that $\tilde{ev}([f(x)]_{q(x)}) = \tilde{ev}([g(x)]_{q(x)})$. This is the same as saying that $\tilde{ev}([f(x)]_{q(x)} - [g(x)]_{q(x)}) = 0$. By definition of \tilde{ev} , we have that $ev(f - g)(c) = 0$ for all c . Therefore, $x, (x - 1), \dots, (x - (p - 1))$ each divide $f(x) - g(x)$. We now claim that for $a \neq b$, $x - a$ is coprime to $x - b$. Indeed, we see that

$$(a - b)^{-1}(x - b) - (a - b)^{-1}(x - a) = 1$$

We further assert that if for some polynomials, $a_1(x) \dots a_n(x)$ mutually coprime, if $a_i(x)|p(x)$ then $a_1(x) \dots a_n(x)|p(x)$. We will prove this by induction. For the case when $n = 2$, this is true by fact 3. Now suppose that it holds for n . We want to show that this is true for $n + 1$. By assumption, $a_1(x) \dots a_n(x)|p(x)$. It is enough to show that $\gcd(a_1(x) \dots a_n(x), a_{n+1}(x)) = 1$. We know that there exists $u_i(x), v_i(x)$ such that $u_i(x)a_i(x) + v_i(x)a_{n+1}(x) = 1$. Multiplying each of these equations together, get

$$\begin{aligned} 1 &= \prod_{i=1}^n (u_i(x)a_i(x) + v_i(x)a_{n+1}(x)) \\ &= P(x)a_1(x) \dots a_n(x) + Q(x)a_{n+1}(x) \end{aligned}$$

For some polynomials $P(x), Q(x)$. Therefore, they are coprime and the claim is proven. Therefore $x(x - 1) \dots (x - (p - 1))|f(x) - g(x)$ and so $x^p - x|f(x) - g(x)$. We can therefore conclude that $[f(x)]_{q(x)} = [g(x)]_{q(x)}$.

Q3d: It is sufficient to show the cardinalities of the domain and co-domain are equal. By A4Q3b, $|\mathbb{F}_p[x]/x^p - x \mathbb{F}_p[x]| = p^p$. We claim the cardinality of $Fun(\mathbb{F}_p, \mathbb{F}_p)$ is the same. Indeed, for $f \in Fun(\mathbb{F}_p, \mathbb{F}_p)$, it will have p possible inputs, and each input has p possible outputs. Therefore there are p^p possible functions. Therefore, we can conclude that \tilde{ev} is a ring isomorphism.

Q3e: Since \tilde{ev} is a bijection it has an inverse. Therefore, for any $g \in Fun(\mathbb{F}_p, \mathbb{F}_p)$, we can apply \tilde{ev}^{-1} to g and get a polynomial in $\mathbb{F}_p[x]/q(x) \mathbb{F}_p[x]$