

Exercise 4.7. Let m a non-negative integer and $z_0, \dots, z_m \in F$ are different to each others, $w_0, \dots, w_m \in F$, show that there is a unique $p \in \mathcal{P}_m(F)$ such that $p(z_k) = w_k$ holds for all $0 \leq k \leq m$.

Proof. Define $\Gamma(p) = (p(z_0), \dots, p(z_m)) : \mathcal{P}_m(F) \rightarrow F^{m+1}$, we will show that Γ is injective, therefore an isomorphism.

Suppose $\Gamma(p) = \Gamma(q)$, then $p(z_k) = q(z_k)$ for all k , therefore $(p - q)(z_k) = 0$ for all k . This means $p - q$ has $m + 1$ zeros but $\deg(p - q) \leq m$, therefore $p - q = 0$ and $p = q$.

Then there is a unique $p \in \mathcal{P}_m(F)$ such that $\Gamma(p) = (w_0, \dots, w_m)$. \square