A.Miller M542
www.math.wisc.edu/∼miller/

Problem 23 *(Wed Mar 5) p is a prime and n a positive integer. Prove:*

(a) If F is a field such that $|F| = p^n$ and m is a positive integer then there is a field E with $F \subseteq E$ and $E = p^{nm}$.

(b) If $F \subseteq E$ are fields, $|F| = p^n$ and $|E| = p^N$, then n divides N.

Proof of (a)

Let $f(x) = x^{p^{nm}} - x$. Let $E_0 \supseteq F$ be a splitting field of $f \in F[x]$ and define

$$E = \{\alpha \in E_0 \;:\; f(\alpha) = 0\}.$$

Then as it was shown in the proof of Theorem 40 E is a field with $|E| = p^{nm}$. It suffices to show that $F \subseteq E$. Note that for any $\alpha \in F$ that $\alpha^{p^n} = \alpha$. It follows that

$$\alpha^{p^{n2}} = \alpha^{p^n \cdot p^n} = (\alpha^{p^n})^{p^n} = (\alpha)^{p^n} = \alpha$$

By an easy induction on k, if $\alpha^{p^n} = \alpha$, then for all k $\alpha^{p^{nk}} = \alpha$.

Proof of (b)

E is a vector space over the field F. If its dimension is m then $|E| = |F|^m$ and so $p^N = (p^n)^m$ and $N = nm$.