Lemma 1: If K is a field of prime characteristic p, positive integers m and k, and $a_1,\ldots,a_k \in K$, then $\left(a_1+a_2+\cdots+a_k\right)^{p^m} = {a_1}^{p^m}+{a_2}^{p^m}+\cdots+{a_k}^{p^m}$

Proof, by induction on k.

The case where k = 1 is the standard rule. The case where k = 2 is proven in notes, pages 38-40. Assume that it is true for all values less than or equal to i, so:

$\left(a_1+a_2+\cdots+a_i\right)^{p^m} = {a_1}^{p^m}+{a_2}^{p^m}+\cdots+{a_i}^{p^m}$

Examine the i+1 case: $\left(a_1+a_2+\cdots+a_i+a_{i+1}\right)^{p^m}$.

Group the last two terms: $\left(a_1+a_2+\cdots+\left(a_i+a_{i+1}\right)\right)^{p^m}$.

Now we have k terms, so: $\left(a_1+a_2+\cdots+\left(a_i+a_{i+1}\right)\right)^{p^m} = {a_1}^{p^m}+{a_2}^{p^m}+\cdots+\left(a_i+a_{i+1}\right)^{p^m}$

The last "term" is just the k=2 case, so:

$\left(a_1+a_2+\cdots+\left(a_i+a_{i+1}\right)\right)^{p^m} = {a_1}^{p^m}+{a_2}^{p^m}+\cdots+{a_i}^{p^m}+{a_{i+1}}^{p^m}$

and we have proven the general statement. ■

Lemma 2: If $a \in GF(p^n) \Leftrightarrow a^{p^n} = a$

Proof:

$(\Rightarrow)$ Assume $a \in GF(p^n)$.

We know that $GF(p^n)$ is the splitting field for the equation $f = t^{p^n} - t$, and f has p^n distinct roots (see page 42 of the notes), and that $GF(p^n)$ has p^n elements (notes pages 44, 48-49), so each element of $GF(p^n)$ is a root of f. Said differently:

$$\left(\forall a \in GF\left(p^n\right)\right) f(a) = a^{p^n} - a = 0 \Rightarrow a^{p^n} = a$$

$(\Leftarrow)$ Assume $a^{p^n} = a$

We know that a is a root of the equation $f = t^{p^n} - t$, which splits over $GF(p^n)$. Hence, we know that $a \in GF(p^n)$. ■

Note that in particular, this finding implies that in $a \in GF(p^1) \approx \mathbb{Z}_p$, $a^p = a$.

Lemma 3: Let $q \in \mathbb{Z}_p[t]$ be an irreducible polynomial over $\mathbb{Z}_p$ of degree m (∂q=m).

$q \mid \left(t^{p^n} - t\right) \Leftrightarrow m \mid n$.

$(\Rightarrow)$ Assume $q \mid \left(t^{p^n} - t\right)$

Recall that $GF(p^n)$ is the splitting field for $t^{p^n} - t$, and that every element in $GF(p^n)$ is a root of this equation. Let α be a root of q over $\mathbb{Z}_p$. q splits in $\mathbb{Z}_p(\alpha) \approx GF(p^m)$, so every root of q is present in both $GF(p^m)$ and $GF(p^n)$ (note, for each root of q, the minimal polynomial of that root divides q, which in turn divides $t^{p^n} - t$. As such, every root of q is also a root of $t^{p^n} - t$, and is thus present in both $GF(p^m)$ and $GF(p^n)$).

This implies that $GF(p^n) : GF(p^m) \approx \mathbb{Z}_p(\alpha)$, which we know implies that $m \mid n$

$(\Leftarrow)$ Assume $m \mid n$

Let α be a root of q over $\mathbb{Z}_p$. This implies that $m_{\alpha,\mathbb{Z}_p} \mid q$. q is irreducible, so $\partial m_{\alpha,\mathbb{Z}_p} = \partial q$, and thus $m_{\alpha,\mathbb{Z}_p}$ and q are associates. We know that $m \mid n$ implies that $GF(p^n) : GF(p^m) \approx \mathbb{Z}_p(\alpha)$. This implies that $\alpha \in GF(p^n)$, and thus that $m_{\alpha,\mathbb{Z}_p} \mid \left(t^{p^n} - t\right)$, which in turn implies that $q \mid \left(t^{p^n} - t\right)$. ■

Theorem: If $q \in \mathbb{Z}_p[t]$, where q is irreducible over $\mathbb{Z}_p$, and ∂q=n , and α is a root of q in some extension of $\mathbb{Z}_p$, then the roots of q in $\mathbb{Z}_p(\alpha) \approx GF(p^n)$ are:

$$\alpha, \alpha^p, \alpha^{p^2}, \alpha^{p^3}, \ldots, \alpha^{p^{n-1}}$$

Proof:

We know that q is of the form $q(t) = b_0 + b_1 t + b_2 t^2 + \cdots + b_n t^n$, where $b_i \in \mathbb{Z}_p$. We know that α is a root of q, so $q(\alpha) = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0$

$q(\alpha) = 0 \Rightarrow q(\alpha)^p = 0^p = 0 = b_0^p + b_1^p(\alpha)^p + b_2^p\left(\alpha^2\right)^p + \cdots + b_n^p\left(\alpha^n\right)^p$ (by lemma 1). Note that $b_i \in \mathbb{Z}_p$, and that $\mathbb{Z}_p$ is a subfield of $\mathbb{Z}_p(\alpha)$. In this subfield, $b_i^p = b_i$ (by lemma 2). So,

$q(\alpha)^p = b_0 + b_1\alpha^p + b_2\alpha^{2p} + \cdots + b_n\alpha^{np} = b_0 + b_1\left(\alpha^p\right) + b_2\left(\alpha^p\right)^2 + \cdots + b_n\left(\alpha^p\right)^n = q(\alpha^p) = 0$,

which implies that α^p is a root of q. Similarly, the values $\alpha^{p^2}, \alpha^{p^3}, \ldots, \alpha^{p^{n-1}}$ are all roots of q. This equations continues to hold for all powers of p, but $\mathbb{Z}_p(\alpha) \approx GF(p^n)$ is finite, so at some point these values will start to repeat.

We will now argue (by contradiction) that each of the listed roots are distinct. Assume that the roots are not distinct. Assume that the first repeated root in the sequence is the kth term, which is equal to the jth term ($0 \le j < k < n$) $\alpha^{p^j} = \alpha^{p^k}$. Raise each side to the power of p^{n-k}. $\left(\alpha^{p^j}\right)^{p^{n-k}} = \left(\alpha^{p^k}\right)^{p^{n-k}} = \alpha^{p^{n+j-k}} = \alpha^{p^n} = \alpha$. This implies that α is a root of the equation of $t^{p^{n+j-k}} - t$, which in turn implies that $m_{\alpha,\mathbb{Z}_p} \mid \left(t^{p^{n+j-k}} - t\right)$. $\partial m_{\alpha,\mathbb{Z}_p} = n$, so $n \mid (n + j - k)$ (by lemma 3), but we have $0 < n - k + j < n$, so n could not divide (n+j-k), yielding a contradiction. ■

References:

Lidl, Rudolf and Niederreiter, Harald. Finite Fields, Second Edition. Copyright 1997. Cambridge University Press. pp 51-53

McEliece, Robert J. Finite Fields for Computer Scientists and Engineers. Copyright 1987. Kluwer Academic Press. pp 44-47.