Recall some facts about finite fields.

- For any prime p, $\mathbb{Z}_p$ is a field with p elements, which we denote $\mathbb{F}_p$.
- Not every finite field has a prime number of elements; for example, we have encountered a finite field with four elements, $\mathbb{F}_4$, in Exercise 4.55.
- However, the number of elements in a finite field must be a *power of a prime*. See Proposition 7.18.

Definition. The **order** of a finite field is the number of elements in the field; it is denoted various ways, e.g. if K is a finite field, its order may be denoted $|K|$ or $\#K$.

Galois' Theorem asserts the *existence* of finite fields of *every* prime power order.

Before proving the theorem, we recall a few more results.

- Every finite field is a field extension of some $\mathbb{F}_p$, where p is a prime, by Proposition 7.15.
- In a field of order $q = p^n$ (where p is prime), every nonzero element a satisfies $a^{q-1} = 1$, by Lemma 7.37. This means that every element a of the field (zero and nonzero) satisfies the equation $a^q - a = 0$. (Check this for yourself.)

Thus to prove the existence of a field with precisely q elements (where q is a prime power, p^n), our strategy is to construct a field extension of $\mathbb{F}_p$ over which the polynomial $x^q - x$ splits, and to prove that the set of roots of $x^q - x$ in this field extension is itself a field, with exactly q elements.

Theorem (Galois)**.** Let p be a prime, and n a positive integer. Then there is a field of order p^n.

Outline of proof. Let $q = p^n$, where p and n are as in the statement of the theorem. Consider the polynomial $g(x) = x^q - x$ in $\mathbb{F}_p[x]$.

By Kronecker's Theorem, there is a field extension K of $\mathbb{F}_p$ over which $x^q - x$ splits.

Let E be the set of roots of $x^q - x$ in K. (This E will be a field with exactly q elements. To prove this, we need to show that E contains exactly q elements and that E is a field.)

To show that E contains exactly q elements, we show that all of the roots of $x^q - x$ are distinct, as follows. (Why does this suffice? See the Factor Theorem (Corollary 6.15) and Theorem 6.16 on page 240.)

We will use the fact that a polynomial that splits over a field K has no repeated roots (i.e. all its roots are distinct) if it is relatively prime to its formal derivative. (See Exercise 6.40(i), on page 263, which in turn relies on the definition of the formal derivative of a polynomial, given in Exercise 5.15, on page 202.)

The formal derivative of $g(x) = x^q - x$ is $g'(x) = q\,x^{q-1} - 1$.

This notation is somewhat misleading, since the coefficients of $g'(x)$ are elements of K, not integers. To be more clear, we might write:

$$g'(x) \;=\; (q\,1_K)x^{q-1} + 1_K,$$

where $q\,1_K = 1_K + 1_K + \cdots + 1_K$ (q times), and 1_K is the multiplicative identity in K. Since $q = p^n$, a small corollary (see below) of Proposition 7.17(i) implies that $q\,1_K = 0_K$. (Having clarified this, we no longer write the subscript "K" on 0 or 1.)

Therefore $g'(x) = qx^{q-1} - 1 = -1$ in $K[x]$, and $\gcd(g, g') = 1$ in $K[x]$, so all the roots of $g(x) = x^q - x$ are distinct. As discussed above, this implies that E has precisely q elements.

Next we show that E is a field, by showing that it is a subring of K (and thus a commutative ring in its own right) and that the multiplicative inverse (in K) of every nonzero element in E lies in E. (See Proposition 4.48.)

To show E is a subring of K, we show that $1 \in E$, and that E is closed under subtraction and multiplication.

Note that for an element a of K to be in E means that $a^q = a$. (Why? Prove this yourself.) It is straightforward to show that $1 \in E$ and that E is closed under multiplication. (Prove these yourself.)

We show that E is closed under subtraction as follows. Take $a, b \in E$; then $a^q = a$ and $b^q = b$. By Proposition 7.17(ii), $(a-b)^q = (a+(-b))^q = a^q + (-b)^q$. If q is odd, then $(-b)^q = -b^q$, so $(a-b)^q = a^q - b^q = a - b$, which implies $a - b \in E$. If q is even, $(-b)^q = b^q$, but since q is a power of a prime, we must have $q = 2^n$ and $\mathbb{F}_p = \mathbb{F}_2$. Thus $-1 = 1$, and $(-b)^q = b^q = -b^q$, implying, as argued above, that $(a-b)^q = a - b$ and $a - b \in E$.

To prove that E is a subfield of K, it is necessary to show that for every nonzero $a \in E$, the multiplicative inverse of a in K, namely a^{-1}, also lies in E. Let $a \neq 0$ be in E. Then $a^q = a$, and, since E is a subring of K, it is a domain, and we may cancel to obtain $a^{q-1} = 1$. Since $q \geq 2$, we have $a \cdot a^{q-2} = 1$ in K, i.e. $a^{-1} = a^{q-2}$ in K. Since E is closed under multiplication and $a \in E$, we have $a^{q-2} \in E$, and thus $a^{-1} \in E$.

Thus E is a field with precisely $q = p^n$ elements, proving the existence of such a field. □

In the proof above, we needed this small consequence of Proposition 7.17(i).

Corollary (of Proposition 7.17(i))**.** Let k be a field of characteristic $p > 0$, and let $q = p^n$ for some positive integer n. Then $qa = 0$ for all $a \in k$.

The proof is left to you as an exercise. Hint: prove that $p^n a = p^{n-1}a + \cdots + p^{n-1}a$ (p times).

Note. Moore's Theorem (Corollary 7.40) says that any two finite fields with the same number of elements are isomorphic. Thus it is usual to refer to *the* finite field with $q = p^n$ elements, since there is only one such field (up to isomorphism), and to denote it as $\mathbb{F}_q$, without any concern of ambiguity. Recall Exercises 4.55 on page 165 and 6.35 on page 263, and see Example 7.41.