

of roots of that equation. Conversely, for every prime power $q = p^f$ the splitting field over \mathbf{F}_p of the polynomial $X^q - X$ is a field of q elements.

Proof. First suppose that \mathbf{F}_q is a finite field. Since the order of any nonzero element divides $q - 1$, it follows that any nonzero element satisfies the equation $X^{q-1} = 1$, and hence, if we multiply both sides by X , the equation $X^q = X$. Of course, the element 0 also satisfies the latter equation. Thus, all q elements of \mathbf{F}_q are roots of the degree- q polynomial $X^q - X$. Since this polynomial cannot have more than q roots, its roots are precisely the elements of \mathbf{F}_q . Notice that this means that \mathbf{F}_q is the splitting field of the polynomial $X^q - X$, that is, the smallest field extension of \mathbf{F}_p which contains all of its roots.

Conversely, let $q = p^f$ be a prime power, and let \mathbf{F} be the splitting field over \mathbf{F}_p of the polynomial $X^q - X$. Note that $X^q - X$ has derivative $qX^{q-1} - 1 = -1$ (because the integer q is a multiple of p and so is zero in the field \mathbf{F}_p); hence, the polynomial $X^q - X$ has no common roots with its derivative (which has no roots at all), and therefore has no multiple roots. Thus, \mathbf{F} must contain at least the q distinct roots of $X^q - X$. But we claim that the set of q roots is already a field. The key point is that a sum or product of two roots is again a root. Namely, if a and b satisfy the polynomial, we have $a^q = a$, $b^q = b$, and hence $(ab)^q = ab$, i.e., the product is also a root. To see that the sum $a + b$ also satisfies the polynomial $X^q - X = 0$, we note a fundamental fact about any field of characteristic p :

Lemma. $(a + b)^p = a^p + b^p$ in any field of characteristic p .

The lemma is proved by observing that all of the intermediate terms vanish in the binomial expansion $\sum_{j=0}^p \binom{p}{j} a^{p-j} b^j$, because $p!/(p-j)!j!$ is divisible by p for $0 < j < p$.

Repeated application of the lemma gives us: $a^p + b^p = (a + b)^p$, $a^{p^2} + b^{p^2} = (a^p + b^p)^p = (a + b)^{p^2}$, ..., $a^q + b^q = (a + b)^q$. Thus, if $a^q = a$ and $b^q = b$ it follows that $(a + b)^q = a + b$, and so $a + b$ is also a root of $X^q - X$. We conclude that the set of q roots is the smallest field containing the roots of $X^q - X$, i.e., the splitting field of this polynomial is a field of q elements. This completes the proof.

In the proof we showed that raising to the p -th power preserves addition and multiplication. We derive another important consequence of this in the next proposition.

Proposition II.1.5. Let \mathbf{F}_q be the finite field of $q = p^f$ elements, and let σ be the map that sends every element to its p -th power: $\sigma(a) = a^p$. Then σ is an automorphism of the field \mathbf{F}_q (a 1-to-1 map of the field to itself which preserves addition and multiplication). The elements of \mathbf{F}_q which are kept fixed by σ are precisely the elements of the prime field \mathbf{F}_p . The f -th power (and no lower power) of the map σ is the identity map.

Proof. A map that raises to a power always preserves multiplication. The fact that σ preserves addition comes from the lemma in the proof of Proposition II.1.4. Notice that for any j the j -th power of σ (the result of