Notice that the element i that we adjoined is *not* a generator of $\mathbf{F}_9^*$, since it has order 4 rather than $q-1=8$. If, however, we adjoin a root α of X^2-X-1, we can get all nonzero elements of $\mathbf{F}_9$ by taking the successive powers of α (remember that α^2 must always be replaced by $\alpha+1$, since α satisfies $X^2=X+1$): $\alpha^1=\alpha$, $\alpha^2=\alpha+1$, $\alpha^3=-\alpha+1$, $\alpha^4=-1$, $\alpha^5=-\alpha$, $\alpha^6=-\alpha-1$, $\alpha^7=\alpha-1$, $\alpha^8=1$. We sometimes say that the polynomial X^2-X-1 is *primitive*, meaning that any root of the irreducible polynomial is a generator of the group of nonzero elements of the field. There are $4=\varphi(8)$ generators of $\mathbf{F}_9^*$, by Proposition II.1.2: two are the roots of X^2-X-1 and two are the roots of X^2+X-1. (The second root of X^2-X-1 is the conjugate of α, namely, $\sigma(\alpha)=\alpha^3=-\alpha+1$.) Of the remaining four nonzero elements, two are the roots of X^2+1 (namely $\pm i=\pm(\alpha+1)$) and the other two are the two nonzero elements ± 1 of $\mathbf{F}_3$ (which are roots of the degree-1 monic irreducible polynomials $X-1$ and $X+1$).

In general, in any finite field $\mathbf{F}_q$, $q=p^f$, each element α satisfies a unique monic irreducible polynomial over $\mathbf{F}_p$ of some degree d. Then the field $\mathbf{F}_p(\alpha)$ obtained by adjoining this element to the prime field is an extension of degree d that is contained in $\mathbf{F}_q$. That is, it is a copy of the field $\mathbf{F}_{p^d}$. Since the big field $\mathbf{F}_{p^f}$ contains $\mathbf{F}_{p^d}$, and so is an $\mathbf{F}_{p^d}$–vector space of some dimension f', it follows that the number of elements in $\mathbf{F}_{p^f}$ must be $(p^d)^{f'}$, i.e., $f=df'$. Thus, $d|f$. Conversely, for any $d|f$ the finite field $\mathbf{F}_{p^d}$ is contained in $\mathbf{F}_q$, because any solution of $X^{p^d}=X$ is also a solution of $X^{p^f}=X$. (To see this, note that for any d', if you repeatedly replace X by X^{p^d} on the left in the equation $X^{p^d}=X$, you can obtain $X^{p^{dd'}}=1$.) Thus, we have proved:

Proposition II.1.7. *The subfields of $\mathbf{F}_{p^f}$ are the $\mathbf{F}_{p^d}$ for d dividing f. If an element of $\mathbf{F}_{p^f}$ is adjoined to $\mathbf{F}_p$, one obtains one of these fields.*

It is now easy to prove a formula that is useful in determining the number of irreducible polynomials of a given degree.

Proposition II.1.8. *For any $q=p^f$ the polynomial X^q-X factors in $\mathbf{F}_p[X]$ into the product of all monic irreducible polynomials of degrees d dividing f.*

Proof. If we adjoin to $\mathbf{F}_p$ a root α of any monic irreducible polynomial of degree $d|f$, we obtain a copy of $\mathbf{F}_{p^d}$, which is contained in $\mathbf{F}_{p^f}$. Since α then satisfies $X^q-X=0$, the monic irreducible must divide that polynomial. Conversely, let $f(X)$ be a monic irreducible polynomial which divides X^q-X. Then $f(X)$ must have its roots in $\mathbf{F}_q$ (since that's where all of the roots of X^q-X are). Thus $f(X)$ must have degree dividing f, by Proposition II.1.7, since adjoining a root gives a subfield of $\mathbf{F}_q$. Thus, the monic irreducible polynomials which divide X^q-X are precisely all of the ones of degree dividing f. Since we saw that X^q-X has no multiple factors, this means that X^q-X is equal to the product of all such irreducible polynomials, as was to be proved.