repeating σ j times) is the map $a \mapsto a^{p^j}$. Thus, the elements left fixed by σ^j are the roots of $X^{p^j} - X$. If $j = 1$, these are precisely the p elements of the prime field (this is the special case $q = p$ of Proposition II.1.4, namely, Fermat's Little Theorem). The elements left fixed by σ^f are the roots of $X^q - X$, i.e., all of $\mathbf{F}_q$. Since the f-th power of σ is the identity map, σ must be 1-to-1 (its inverse map is $\sigma^{f-1}: \ a \mapsto a^{p^{f-1}}$). No lower power of σ gives the identity map, since for $j < f$ not all of the elements of $\mathbf{F}_q$ could be roots of the polynomial $X^{p^j} - X$. This completes the proof.

Proposition II.1.6. *In the notation of Proposition II.1.5, if α is any element of $\mathbf{F}_q$, then the conjugates of α over $\mathbf{F}_p$ (the elements of $\mathbf{F}_q$ which satisfy the same monic irreducible polynomial with coefficients in $\mathbf{F}_p$) are the elements $\sigma^j(\alpha) = \alpha^{p^j}$.*

Proof. Let d be the degree of $\mathbf{F}_p(\alpha)$ as an extension of $\mathbf{F}_p$. That is, $\mathbf{F}_p(\alpha)$ is a copy of $\mathbf{F}_{p^d}$. Then α satisfies $X^{p^d} - X$ but does not satisfy $X^{p^j} - X$ for any $j < d$. Thus, one obtains d distinct elements by repeatedly applying σ to α. It now suffices to show that each of these elements satisfies the same monic irreducible polynomial $f(X)$ that α does, in which case they must be the d roots. To do this, it is enough to prove that, if α satisfies a polynomial $f(X) \in \mathbf{F}_p[X]$, then so does α^p. Let $f(X) = \sum a_j X^j$, where $a_j \in \mathbf{F}_p$. Then $0 = f(\alpha) = \sum a_j \alpha^j$. Raising both sides to the p-th power gives $0 = \sum (a_j \alpha^j)^p$ (where we use the fact that raising a sum $a + b$ to the p-th power gives $a^p + b^p$). But $a_j^p = a_j$, by Fermat's Little Theorem, and so we have: $0 = \sum a_j (\alpha^p)^j = f(\alpha^p)$, as desired. This completes the proof.

Explicit construction. So far our discussion of finite fields has been rather theoretical. Our only practical experience has been with the finite fields of the form $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. We now discuss how to work with finite extensions of $\mathbf{F}_p$. At this point we should recall how in the case of the rational numbers $\mathbf{Q}$ we work with an extension such as $\mathbf{Q}(\sqrt{2})$. Namely, we get this field by taking a root α of the equation $X^2 - 2$ and looking at expressions of the form $a + b\alpha$, which are added and multiplied in the usual way, except that α^2 should always be replaced by 2. (In the case of $\mathbf{Q}(\sqrt[3]{2})$ we work with expressions of the form $a + b\alpha + c\alpha^2$, and when we multiply we always replace α^3 by 2.) We can take the same general approach with finite fields.

Example 2. To construct $\mathbf{F}_9$ we take any monic quadratic polynomial in $\mathbf{F}_3[X]$ which has no roots in $\mathbf{F}_3$. By trying all possible choices of coefficients and testing whether the elements $0, \pm 1 \in \mathbf{F}_3$ are roots, we find that there are three monic irreducible quadratics: $X^2 + 1$, $X^2 \pm X - 1$. If, for example, we take α to be a root of $X^2 + 1$ (let's call it i rather than α — after all, we are simply adjoining a square root of -1), then the elements of $\mathbf{F}_9$ are all combinations $a + bi$, where a and b are 0, 1, or -1. Doing arithmetic in $\mathbf{F}_9$ is thus a lot like doing arithmetic in the Gaussian integers (see Exercise 14 of § I.2), except that our arithmetic with the coefficients a and b occurs in the tiny field $\mathbf{F}_3$.