Fact: (Professor Lubin) If you want to find the inverse of some polynomial f(x) in a simple field extension k(alpha), it's equivalent to find the inverse of the matrix of the linear operator f(T), where T is the multiplication by alpha map T : k(alpha) \to k(alpha) that sends x to alpha x.

Ex.: f(x) = x^3 - 9x + 3 is 3-Eisenstein and hence irreducible over Q. January 2017, Q4

$$\mathcal{B} = \{1, \alpha, \alpha^2\}$$

$$[T]_{\mathcal{B}} = \begin{array}{ccc} \multicolumn{3}{c}{\begin{pmatrix} 0 & 0 & -3 \\ 1 & 0 & 9 \\ 0 & 1 & 0 \end{pmatrix}} \\ 1 \mapsto \alpha & \alpha \mapsto \alpha^2 & \alpha^2 \mapsto \alpha^3 = 9\alpha - 3 \end{array} = C_{f(x)} = A$$

$$(3\alpha^2 + 2\alpha + 1)^{-1} \leftrightarrow (3A^2 + 2A + I)^{-1} = \frac{-1}{1507}(80A^2 + 29A - 766I)$$

One can also use WolframAlpha to find the inverse of a matrix. For our example, define the matrix A = {(0,0,-3), (1,0,9), (0,1,0)} and the 3 x 3 identity matrix I = {(1,0,0), (0,1,0), (0,0,1)} in WolframAlpha. Then, use the command (3A^2 + 2A + I)^(-1) to find the inverse matrix.

January 2015, Q4

$\alpha = \sqrt{2} + \sqrt[3]{2}$

Because 2 and 3 are relatively prime, we expect that [Q(alpha) : Q] = 6, i.e., the minimal polynomial has degree 6. If we can find a monic polynomial p(x) of degree six for which alpha is a root, then arguing that [Q(alpha) : Q] = 6, we will be done: p(x) is the minimal polynomial.

a - sqrt(2) = sqrt[3](2)
(a - sqrt(2))^3 = 2
a^3 - 3 sqrt(2) a^2 + 6a - 2 sqrt(2) = 2
a^3 - 3 sqrt(2) a^2 + 6a - 2 sqrt(2) - 2 = 0
conjugate
(a^3 - 3 sqrt(2) a^2 + 6a - 2 sqrt(2) - 2)(a^3 + 3 sqrt(2) a^2 + 6a + 2 sqrt(2) - 2) = 0
a^6 - 6a^4 - 4a^3 + 12a^2 - 24a - 4 = 0

p(x) = x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4 has alpha (a) as a root.

Claim: p(x) is the minimal polynomial of alpha.

Proof. If [Q(alpha) : Q] = 6, then p(x) has to be the minimal polynomial of alpha.

?
[Q(sqrt(2), sqrt[3](2)) : Q] = [Q(sqrt[3](2)) : Q(sqrt(2))][Q(sqrt(2)) : Q] = 3*2 = 6

Claim: Q(alpha) = Q(sqrt(2), sqrt[3](2))

alpha = sqrt(2) + sqrt[3](2), so Q(alpha) is contained in Q(sqrt(2), sqrt[3](2)).

By our previous computation (star), we have that a^3 + 6a - 2 = sqrt(2)(3a^2 + 2). But Q(alpha) is a field, so we may divide both sides by 3a^2 + 2, which shows that sqrt(2) is contained in Q(alpha). So, then, sqrt[3](2) = a - sqrt(2) is in Q(alpha).

Last, we must verify that [Q(sqrt[3](2)) : Q(sqrt(2))] = 3. The claim is that x^3 - 2 is the minimal polynomial of sqrt[3](2) over Q(sqrt(2)). If it's not irreducible, then it has a linear factor x - sqrt[3](2), i.e., sqrt[3](2) belongs to Q(sqrt(2)). By definition, then, there exist some rational numbers a and b such that sqrt[3](2) = a + b sqrt(2).

Cubing both sides and using that sqrt[3](2) = a + b sqrt(2), we find that sqrt(2) is a rational number — a contradiction. So, x^3 - 2 is the minimal polynomial of sqrt[3](2) over Q(sqrt(2)).