Solving the Cubic

Let $f(x) = x^3 - ax^2 + bx - c$ be an irreducible cubic in $F[x]$. Assume char $F \neq 2$ or 3. The Galois group is either S_3 or A_3. Setting $g(x) = f(x + a/3)$, note $g(x) = x^3 + px - q$. Roots r, s, t of $g(x)$ are obtained by subtracting $a/3$ from roots of $f(x)$, so they have the same splitting field. Also, the discriminants of $f(x)$ and $g(x)$ are the same, where the discriminant, D, is given by $D = (r-s)^2(s-t)^2(t-r)^2$ with $\sqrt{D} = d = (r-s)(s-t)(t-r) = r^2t + t^2s + s^2r - r^2s - s^2t - t^2r$.

Now D is invariant under S_3 hence must be in the ground field F. However d changes sign under a transposition of two roots. As a corollary, the Galois group of $f(x)$ is A_3 if and only if D is a square in F.

We show that $D = -4p^3 - 27q^2$. There are various clever proofs of this formula, see Lang for one, but a not so clever proof is just to expand D, write D in terms of the elementary symmetric functions in r, s, t, and use $r + s + t = 0$, $rs + st + tr = p$, and $rst = q$.

Now let ζ denote a primitive cube root of 1. We have the Lagrange resolvants, whose cubes are in F:

$$u = r + s + t = 0, \quad v = r + \zeta s + \zeta^2 t, \quad w = r + \zeta^2 s + \zeta t$$

Note $3r = u + v + w = v + w$, since $1 + \zeta + \zeta^2 = 0$. Also, a computation gives $vw = -3p$. We thus have a formula for the root r of $g(x)$ once we find v^3 and w^3. Computation gives:

$$v^3 = r^3 + s^3 + t^3 + 6rst + 3\zeta(r^2s + s^2t + t^2r) + 3\zeta^2(r^2t + t^2s + s^2r),$$
$$w^3 = r^3 + s^3 + t^3 + 6rst + 3\zeta^2(r^2s + s^2t + t^2r) + 3\zeta(r^2t + t^2s + s^2r).$$

Taking $\zeta = (-1 + \sqrt{-3})/2$ and $\zeta^2 = (-1 - \sqrt{-3})/2$ and using the above 'symmetric' formula for $d = \sqrt{D}$, we get

$$v^3 + w^3 = 27q \quad \text{and} \quad v^3 - w^3 = (-3\sqrt{-3})\sqrt{D},$$

where the first simplification results from $r + s + t = 0$ used a few times. Solving and using the above explicit formula for D:

$$v^3 = \frac{27q - (3\sqrt{-3})\sqrt{D}}{2} = \frac{27q - (3\sqrt{-3})\sqrt{-4p^3 - 27q^2}}{2},$$
$$w^3 = \frac{27q + (3\sqrt{-3})\sqrt{D}}{2} = \frac{27q + (3\sqrt{-3})\sqrt{-4p^3 - 27q^2}}{2}$$

$r = v + w$ gives a formula for one root of $g(x)$ as 1/3 the sum of two cube roots of elements of $F[\sqrt{D}]$. This is Cardan's formula, as derived by Lagrange. The cube roots v and w are not independent since $vw = -3p$. One gets the other two conjugates s and t of r by reinterpreting the cube roots v, w, keeping the product $vw = -3p$:

$$3r = v + w, \qquad 3s = \zeta v + \zeta^2 w, \qquad 3t = \zeta^2 v + \zeta w.$$

Solving the quartic is harder. The composition series for S_4 is $S_4 > A_4 > V_4 > C_2 > 1$. The Galois group is reduced to A_4 by adjoining the square root of the discriminant, which is not a pretty sight for a quartic. If the four roots are r, s, t, u then the element $rs + tu$ is invariant under $V_4 = \{1, (rs)(tu), (rt)(su), (ru)(st)\}$. Its conjugates under A_4 are $rs + tu$, $rt + su$, and $ru + st$. These three elements are roots of a cubic over $F[\sqrt{D}]$, which can be computed explicitly and solved with the Cardan formulas. This gives the fixed field of V_4. If $C_2 = \{1, (rs)(tu)\}$ then elements rs and $r + s$ are in the fixed field of C_2. Their V_4 conjugates are tu and $t + u$, respectively, and one can find all these elements by solving quadratic equations over the fixed field of V_4. This gives the fixed field of C_2. Finally, one finds r, s, t, u by solving quadratic equations over the fixed field of C_2. There are some books that carry all this out explicitly.