The discriminant D for this cubic is

$$D = -4(-21)^3 - 27(-7)^2 = 3^6 7^2$$

which shows that the Galois group for this (Eisenstein at 7) cubic is A_3. Substituting into the formulas above we have

$$A = 3\sqrt[3]{\frac{7}{2} + \frac{21}{2}\sqrt{-3}}$$

$$B = 3\sqrt[3]{\frac{7}{2} - \frac{21}{2}\sqrt{-3}}$$

and the roots of our cubics can be expressed in terms of A and B using the formulas above. This cubic arises from trying to express a primitive 7^{th} root of unity ζ_7 in terms of radicals similar to the explicit formulas for the other roots of unity of small order (cf. the exercises).

In this case we have $g(-5) = -27$, $g(-1) = 13$, $g(0) = -7$ and $g(5) = 13$, so that this cubic has 3 *real* roots. The expressions above for these roots are sums of the conjugates of *complex* numbers. We shall see later that this is necessary, namely that it is impossible to solve for these real roots using only radicals involving real numbers.

A cubic with rational coefficients has either one real root and two complex conjugate imaginary roots or has three real roots. These two cases can be distinguished by the sign of the discriminant:

Suppose in the first case that the roots are a and $b \pm ic$ where a, b, and c are real and $c \neq 0$. Then

$$\begin{aligned}\sqrt{D} &= [a - (b + ic)][a - (b - ic)][(b + ic) - (b - ic)] \\ &= 2ic[(a - b)^2 + c^2]\end{aligned}$$

is purely imaginary, so that the discriminant D is negative. Then in the formulas for A and B above we may choose both to be real. The first root in (27) is then real and the second two are complex conjugates.

If all three roots are real, then clearly $\sqrt{D}$ is real, so $D \geq 0$ is a nonnegative real number. If $D = 0$ then the cubic has repeated roots. For $D > 0$ (sometimes called the *Casus irreducibilis*), the formulas for the roots involve radicals of nonreal numbers, as in Example 2. We now show that for irreducible cubics this is necessary. The exercises outline the proof of the following generalization: if all the roots of the irreducible polynomial $f(x) \in \mathbb{Q}[x]$ are real and if one of these roots can be expressed by *real* radicals, then the degree of $f(x)$ is a power of 2, the Galois group of $f(x)$ is a 2-group, and the roots of $f(x)$ can be constructed by straightedge and compass.

Suppose that the irreducible cubic $f(x)$ has three real roots and that it were possible to express one of these roots by radicals involving only real numbers. Then the splitting field for the cubic would be contained in a root extension

$$\mathbb{Q} = K_0 \subset K_1 = \mathbb{Q}(\sqrt{D}) \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_s = K$$

where each field K_i, $i = 0, 1, \ldots, s$, is contained in the real numbers $\mathbb{R}$ and $s \geq 2$ since the quadratic extension $\mathbb{Q}(\sqrt{D})$ cannot contain the root of an irreducible cubic. We have begun this root extension with $\mathbb{Q}(\sqrt{D})$ because over this field the Galois group of the polynomial is cyclic of degree 3.

Note that for any field F the extension $F(\sqrt[mn]{a})$ of F can be obtained by two smaller simple radical extensions: let

$$F_1 = F(\sqrt[n]{a})$$

and let $b = \sqrt[n]{a} \in F_1$, so that

$$F(\sqrt[mn]{a}) = F_1(\sqrt[m]{b}).$$

We may therefore always assume our radical extensions are of the form $F(\sqrt[p]{a})$ where p is a prime.

Suppose now that F is a subfield of the real numbers $\mathbb{R}$ and let a be an element of F. Let p be a prime and let $\alpha = \sqrt[p]{a}$ denote a real p^{th} root of a. Then $[F(\sqrt[p]{a}) : F]$ must be either 1 or p, as follows. The conjugates of α over F all differ from α by a p^{th} root of unity. It follows that the constant term of the minimal polynomial of α over F is $\alpha^d\zeta$ where $d = [F(\sqrt[p]{a}) : F]$ is the degree of the minimal polynomial and ζ is some p^{th} root of unity. Since α is real and $\alpha^d\zeta \in F$ is real, it follows that $\zeta = \pm 1$, so that $\alpha^d \in F$. Then, if $d \neq p$, $\alpha^d \in F$ and $\alpha^p = a \in F$ implies $\alpha \in F$, so $d = 1$.

Hence we may assume for the radical extensions above that $[K_{i+1} : K_i]$ is a prime p_i and $K_{i+1} = K_i(\sqrt[p_i]{a_i})$ for some $a_i \in K_i$, $i = 0, 1, \ldots, s-1$. In other words, the original tower of real radical extensions can be refined to a tower where each of the successive radical extensions has prime degree.

If any field containing $\sqrt{D}$ contains one of the roots of $f(x)$ then it contains the splitting field for $f(x)$, hence contains all the roots of the cubic. We suppose s is chosen so that K_{s-1} does not contain any of the roots of the cubic.

Consider the extension K_s/K_{s-1}. The field K_s contains all the roots of the cubic $f(x)$ and the field K_{s-1} contains none of these roots. It follows that $f(x)$ is irreducible over K_{s-1}, so $[K_s : K_{s-1}]$ is divisible by 3. Since we have reduced to the case where this extension degree is a prime, it follows that the extension degree is precisely 3 and that the extension K_s/K_{s-1} is Galois (being the splitting field of $f(x)$ over K_{s-1}). Since also $K_s = K_{s-1}(\sqrt[3]{a})$ for some $a \in K_{s-1}$, the Galois extension K_s must also contain the other cube roots of a. This implies that K_s contains ρ, a primitive 3^{rd} root of unity. This contradicts the assumption that K_s is a subfield of $\mathbb{R}$ and shows that it is impossible to express the roots of this cubic in terms of real radicals only.

Solution of Quartic Equations by Radicals

Consider now the case of a quartic polynomial

$$f(x) = x^4 + ax^3 + bx^2 + cx + d$$

which under the substitution $x = y - a/4$ becomes the quartic

$$g(y) = y^4 + py^2 + qy + r$$

with

$$p = \frac{1}{8}(-3a^2 + 8b)$$

$$q = \frac{1}{8}(a^3 - 4ab + 8c)$$

$$r = \frac{1}{256}(-3a^4 + 16a^2b - 64ac + 256d).$$

Let the roots of $g(y)$ be α_1, α_2, α_3, and α_4. The resolvent cubic introduced in the previous section for this quartic is

$$h(x) = x^3 - 2px^2 + (p^2 - 4r)x + q^2$$

and has roots

$$\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$$
$$\theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$$
$$\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3).$$

The Galois group of the splitting field for $f(x)$ (or $g(y)$) over the splitting field of the resolvent cubic $h(x)$ is the Klein 4-group. Such extensions are biquadratic, which means that it is possible to solve for the roots α_1, α_2, α_3, and α_4 in terms of square roots of expressions involving the roots θ_1, θ_2, and θ_3 of the resolvent cubic. In this case we evidently have

$$(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = \theta_1 \qquad (\alpha_1 + \alpha_2) + (\alpha_3 + \alpha_4) = 0$$

which gives

$$\alpha_1 + \alpha_2 = \sqrt{-\theta_1} \qquad \alpha_3 + \alpha_4 = -\sqrt{-\theta_1}.$$

Similarly,

$$\alpha_1 + \alpha_3 = \sqrt{-\theta_2} \qquad \alpha_2 + \alpha_4 = -\sqrt{-\theta_2}$$
$$\alpha_1 + \alpha_4 = \sqrt{-\theta_3} \qquad \alpha_2 + \alpha_3 = -\sqrt{-\theta_3}.$$

An easy computation shows that $\sqrt{-\theta_1}\sqrt{-\theta_2}\sqrt{-\theta_3} = -q$, so that the choice of two of the square roots determines the third. Since $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, if we add the left-hand equations above we obtain $2\alpha_1$, and similarly we may solve for the other roots of $g(y)$. We find

$$2\alpha_1 = \sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3}$$
$$2\alpha_2 = \sqrt{-\theta_1} - \sqrt{-\theta_2} - \sqrt{-\theta_3}$$
$$2\alpha_3 = -\sqrt{-\theta_1} + \sqrt{-\theta_2} - \sqrt{-\theta_3}$$
$$2\alpha_4 = -\sqrt{-\theta_1} - \sqrt{-\theta_2} + \sqrt{-\theta_3}$$

which reduces the solution of the quartic equation to the solution of the associated resolvent cubic.

EXERCISES

1. Use Cardano's Formulas to solve the equation $x^3 + x^2 - 2 = 0$. In particular show that the equation has the real root

$$\frac{1}{3}(\sqrt[3]{26 + 15\sqrt{3}} + \sqrt[3]{26 - 15\sqrt{3}} - 1).$$

Show directly that the roots of this cubic are $1, -1 \pm i$. Explain this by proving that

$$\sqrt[3]{26 + 15\sqrt{3}} = 2 + \sqrt{3} \quad \sqrt[3]{26 - 15\sqrt{3}} = 2 - \sqrt{3}$$

so that

$$\sqrt[3]{26+15\sqrt{3}}+\sqrt[3]{26-15\sqrt{3}}=4.$$

2. Let ζ_7 be a primitive 7^{th} root of unity and let $\alpha=\zeta+\zeta^{-1}$.
   (a) Show that ζ_7 is a root of the quadratic $z^2-\alpha z+1$ over $\mathbb{Q}(\alpha)$.
   (b) Show using the minimal polynomial for ζ_7 that α is a root of the cubic x^3+x^2-2x-1.
   (c) Use (a) and (b) together with the explicit solution of the cubic in (b) in the text to express ζ_7 in terms of radicals similar to the expressions given earlier for the other roots of unity of small order. (The complicated nature of the expression explains why we did not include ζ_7 earlier in our list of explicit roots of unity.)
3. Let F be a field of characteristic $\neq 2$. State and prove a necessary and sufficient condition on $\alpha, \beta \in F$ so that $F(\sqrt{\alpha})=F(\sqrt{\beta})$. Use this to determine whether $\mathbb{Q}(\sqrt{1-\sqrt{2}})=\mathbb{Q}(i,\sqrt{2})$.
4. Let $K=\mathbb{Q}(\sqrt[n]{a})$, where $a\in\mathbb{Q}, a>0$ and suppose $[K:\mathbb{Q}]=n$ (i.e., x^n-a is irreducible). Let E be any subfield of K and let $[E:\mathbb{Q}]=d$. Prove that $E=\mathbb{Q}(\sqrt[d]{a})$. [Consider $N_{K/E}(\sqrt[n]{a})\in E$.]
5. Let K be as in the previous exercise. Prove that if n is odd then K has no nontrivial subfields which are Galois over $\mathbb{Q}$ and if n is even then the only nontrivial subfield of K which is Galois over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{a})$.
6. Let L be the Galois closure of K in the previous two exercises (i.e., the splitting field of x^n-a). Prove that $[L:\mathbb{Q}]=n\varphi(n)$ or $\frac{1}{2}n\varphi(n)$. [Note that $\mathbb{Q}(\zeta_n)\cap K$ is a Galois extension of $\mathbb{Q}$.]
7. (*Kummer Generators for Cyclic Extensions*) Let F be a field of characteristic not dividing n containing the n^{th} roots of unity and let K be a cyclic extension of degree d dividing n. Then $K=F(\sqrt[n]{a})$ for some nonzero $a\in F$. Let σ be a generator for the cyclic group $\text{Gal}(K/F)$.
   (a) Show that $\sigma(\sqrt[n]{a})=\zeta\sqrt[n]{a}$ for some primitive d^{th} root of unity ζ.
   (b) Suppose $K=F(\sqrt[n]{a})=F(\sqrt[n]{b})$. Use (a) to show that $\dfrac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}=\left(\dfrac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}\right)^i$ for some integer i relatively prime to d. Conclude that σ fixes the element $\dfrac{\sqrt[n]{a}}{(\sqrt[n]{b})^i}$ so this is an element of F.
   (c) Prove that $K=F(\sqrt[n]{a})=F(\sqrt[n]{b})$ if and only if $a=b^ic^n$ and $b=a^jd^n$ for some $c,d\in F$, i.e., if and only if a and b generate the same subgroup of $F^\times$ modulo n^{th} powers.
8. Let p, q and r be primes in $\mathbb{Z}$ with $q\neq r$. Let $\sqrt[p]{q}$ denote any root of x^p-q and let $\sqrt[p]{r}$ denote any root of x^p-r. Prove that $\mathbb{Q}(\sqrt[p]{q})\neq\mathbb{Q}(\sqrt[p]{r})$.
9. (*Artin–Schreier Extensions*) Let F be a field of characteristic p and let K be a cyclic extension of F of degree p. Prove that $K=F(\alpha)$ where α is a root of the polynomial x^p-x-a for some $a\in F$. [Note that $\text{Tr}_{K/F}(-1)=0$ since F is of characteristic p so that $-1=\alpha-\sigma\alpha$ for some $\alpha\in K$ where σ is a generator of $\text{Gal}(K/F)$ by Exercise 26 of Section 2. Show that $a=\alpha^p-\alpha$ is an element of F.] Note that since F contains the p^{th} roots of unity (namely, 1) that this completes the description of all cyclic extensions of prime degree p over fields containing the p^{th} roots of unity in all characteristics.
10. Let $K=\mathbb{Q}(\zeta_p)$ be the cyclotomic field of p^{th} roots of unity for the prime p and let