$G = \mathrm{Gal}(K/\mathbb{Q})$. Let ζ denote any p^{th} root of unity. Prove that $\sum_{\sigma \in G} \sigma(\zeta)$ (the trace from K to $\mathbb{Q}$ of ζ) is -1 or $p-1$ depending on whether ζ is or is not a primitive p^{th} root of unity.

11. (*The Classical Gauss Sum*) Let $K = \mathbb{Q}(\zeta_p)$ be the cyclotomic field of p^{th} roots of unity for the odd prime p, viewed as a subfield of $\mathbb{C}$, and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Let H denote the subgroup of index 2 in the cyclic group G. Define $\eta_0 = \sum_{\tau \in H} \tau(\zeta_p)$, $\eta_1 = \sum_{\tau \in \sigma H} \tau(\zeta_p)$, where σ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$ (the two *periods* of ζ_p with respect to H, i.e., the sum of the conjugates of ζ_p with respect to the two cosets of H in G, cf. Section 5).

(a) Prove that $\sigma(\eta_0) = \eta_1$, $\sigma(\eta_1) = \eta_0$ and that

$$\eta_0 = \sum_{a = \text{square}} \zeta_p^a \quad , \quad \eta_1 = \sum_{b \neq \text{square}} \zeta_p^b,$$

where the sums are over the squares and nonsquares (respectively) in $(\mathbb{Z}/p\mathbb{Z})^\times$. [Observe that H is the subgroup of squares in $(\mathbb{Z}/p\mathbb{Z})^\times$.]

(b) Prove that $\eta_0 + \eta_1 = (\zeta_p, 1) = -1$ and $\eta_0 - \eta_1 = (\zeta_p, -1)$ where $(\zeta_p, 1)$ and $(\zeta_p, -1)$ are two of the Lagrange resolvents of ζ_p.

(c) Let $g = \sum_{i=0}^{p-1} \zeta_p^{i^2}$ (the classical *Gauss sum*). Prove that

$$g = (\zeta_p, -1) = \sum_{i=0}^{p-2} (-1)^i \sigma^i(\zeta_p).$$

(d) Prove that $\tau g = g$ if $\tau \in H$ and $\tau g = -g$ if $\tau \notin H$. Conclude in particular that $[\mathbb{Q}(g) : \mathbb{Q}] = 2$. Recall that complex conjugation is the automorphism σ_{-1} on K (cf. Exercise 7 of Section 5). Conclude that $\bar{g} = g$ if -1 is a square mod p (i.e., if $p \equiv 1 \bmod 4$) and $\bar{g} = -g$ if -1 is not a square mod p (i.e., if $p \equiv 3 \bmod 4$) where $\bar{g}$ denotes the complex conjugate of g.

(e) Prove that $g\bar{g} = p$. [The complex conjugate of a root of unity is its reciprocal. Then $\bar{g} = \sum_{j=0}^{p-2} (-1)^j (\sigma^j(\zeta_p))^{-1}$ gives

$$g\bar{g} = \sum_{i,j=0}^{p-2} (-1)^i (-1)^j \frac{\sigma^i(\zeta_p)}{\sigma^j(\zeta_p)} = \sum_{i,j=0}^{p-2} (-1)^{i-j} \sigma^j \left[\frac{\sigma^{i-j}(\zeta_p)}{\zeta_p} \right]$$

$$= \sum_{k=0}^{p-2} (-1)^k \sum_{j=0}^{p-2} \sigma^j \left[\frac{\sigma^k(\zeta_p)}{\zeta_p} \right]$$

where $k = i - j$. If $k = 0$ the element $\dfrac{\sigma^k(\zeta_p)}{\zeta_p}$ is 1, and if $k \neq 0$ then this is a primitive p^{th} root of unity. Use the previous exercise to conclude that the inner sum is $p - 1$ when $k = 0$ and is -1 otherwise.]

(f) Conclude that $g^2 = (-1)^{(p-1)/2} p$ and that $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2} p}\,)$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$. (Cf. also Exercise 33 of Section 6.)

12. Let L be the Galois closure of the finite extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$. For any prime p dividing the order of $\mathrm{Gal}(L/\mathbb{Q})$ prove there is a subfield F of L with $[L : F] = p$ and $L = F(\alpha)$.

13. Let F be a subfield of the real numbers $\mathbb{R}$. Let a be an element of F and let $K = F(\sqrt[n]{a})$ where $\sqrt[n]{a}$ denotes a real n^{th} root of a. Prove that if L is any Galois extension of F contained in K then $[L : F] \leq 2$.

14. This exercise shows that in general it is necessary to use complex numbers when expressing real roots in terms of radicals and generalizes the *Casus irreducibilis* of cubic equations.

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial all of whose roots are real. Suppose further that one of the roots, α, of $f(x)$ can be expressed in terms of *real* radicals (i.e., there is a root extension of real fields $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_m \subset \mathbb{R}$ with $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, $i = 1, 2, \ldots, m-1$, for some integers n_i and some $a_i \in K_i$ and $\alpha \in K_m$). Prove that the Galois group of $f(x)$ is a 2-group. Conclude in particular that the degree of $f(x)$ is a power of 2 and that the real roots of such a polynomial can be expressed entirely in terms of real radicals if and only if these roots can be constructed by straightedge and compass. [The argument is similar to the case of cubics. Let $L \in \mathbb{R}$ be the Galois closure of $\mathbb{Q}(\alpha)$ and suppose the order of $\mathrm{Gal}(L/\mathbb{Q})$ is divisible by some odd prime p. Let F be a subfield of L with $[L : F] = p$ and $L = F(\alpha)$ (by Exercise 12) and consider the composite fields $K_i' = FK_i$, $i = 0, 1, \ldots, m$. These are again real radical extensions and by the argument in the text for the *Casus irreducibilis*, we may assume each $[K_{i+1}' : K_i']$ is a prime. Since $\alpha \notin F = FK_0$, there is an integer s with $\alpha \notin K_{s-1}'$, $\alpha \in K_s'$. Since the extensions are of prime degree, we have $K_s' = K_{s-1}'(\alpha)$. Since $L = F(\alpha)$ is Galois of degree p, K_s' is a Galois extension of K_{s-1}' of degree p, contradicting the previous exercise.]

15. *('Cardano's Formulas' for a Cubic in Characteristic 2)* Suppose $f(x) = x^3 + px + q$ is an irreducible cubic over a field of characteristic 2. Let ρ be a primitive 3rd root of unity and let θ, θ' be the roots of the quadratic $x^2 + qx + (p^3 + q^2)$ (cf. Exercise 50 of Section 6). Let θ_1 and θ_2 be cube roots of $\rho q + \theta$ and $\rho q + \theta'$, respectively, where the cube roots are chosen so that $\theta_1\theta_2 = p$. Prove that the roots of $f(x)$ are given by $\alpha = \theta_1 + \theta_2$, $\beta = \rho\alpha + \theta_1$, and $\gamma = \rho\alpha + \theta_2 = \alpha + \beta$.

16. Let a be a nonzero rational number.

(a) Determine when the extension $\mathbb{Q}(\sqrt{ai})$ ($i^2 = -1$) is of degree 4 over $\mathbb{Q}$.

(b) When $K = \mathbb{Q}(\sqrt{ai})$ is of degree 4 over $\mathbb{Q}$ show that K is Galois over $\mathbb{Q}$ with the Klein 4-group as Galois group. In this case determine the quadratic extensions of $\mathbb{Q}$ contained in K.

17. Let $D \in \mathbb{Z}$ be a squarefree integer and let $a \in \mathbb{Q}$ be a nonzero rational number. Show that $\mathbb{Q}(\sqrt{a\sqrt{D}})$ cannot be a cyclic extension of degree 4 over $\mathbb{Q}$.

18. Let $D \in \mathbb{Z}$ be a squarefree integer and let $a \in \mathbb{Q}$ be a nonzero rational number. Prove that if $\mathbb{Q}(\sqrt{a\sqrt{D}})$ is Galois over $\mathbb{Q}$ then $D = -1$.

19. Let $D \in \mathbb{Z}$ be a squarefree integer and let $K = \mathbb{Q}(\sqrt{D})$.

(a) Prove that if $D = s^2 + t^2$ is the sum of two rational squares then there exists an extension $L/\mathbb{Q}$ containing K which is Galois over $\mathbb{Q}$ with a cyclic Galois group of order 4. [Consider the extension $\mathbb{Q}(\sqrt{D + s\sqrt{D}})$.] (Note also that D is the sum of two rational squares if and only if D is also the sum of two integer squares, so one may assume s and t are integral without loss.)

(b) Prove conversely that if K can be embedded in a cyclic extension L of degree 4 as in (a) then D is the sum of two squares. [One approach: (i) observe first that L is quadratic over K, so $L = K(\sqrt{a + b\sqrt{D}})$ for some $a, b \in \mathbb{Q}$, (ii) show that L contains the quadratic subfield $\mathbb{Q}(\sqrt{a^2 - b^2D})$, which must be $\mathbb{Q}(\sqrt{D})$ if $L/\mathbb{Q}$ is cyclic, and use Exercise 7.]

(c) Conclude in particular that $\mathbb{Q}(\sqrt{3})$ is not a subfield of any cyclic extension of degree 4 over $\mathbb{Q}$. Similarly conclude that the fields $\mathbb{Q}(\sqrt{D})$ for squarefree integers $D < 0$ are never contained in cyclic extensions of degree 4 over $\mathbb{Q}$ (this gives an alternate proof for Exercise 19, Section 6).

20. Let p be a prime. Show that any solvable subgroup of S_p of order divisible by p is

contained in the normalizer of a Sylow p-subgroup of S_p (a Frobenius group of order $p(p-1)$). Conclude that an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree p is solvable by radicals if and only if its Galois group is contained in the Frobenius group of order $p(p-1)$. [Let $G \leq S_p$ be a solvable subgroup of order divisible by p. Then G contains a p-cycle, hence is transitive on $\{1, 2, \ldots, p\}$. Let $H < G$ be the stabilizer in G of the element 1, so H has index p in G. Show that H contains no nontrivial normal subgroups of G (note that the conjugates of H are the stabilizers of the other points). Let $G^{(n-1)}$ be the last nontrivial subgroup in the derived series for G. Show that $H \cap G^{(n-1)} = 1$ and conclude that $|G^{(n-1)}| = p$, so that the Sylow p-subgroup of G (which is also a Sylow p-subgroup in S_p) is normal in G.]

21. (*Criterion for the Solvability of a Quintic*) By the previous exercise, an irreducible polynomial $f(x)$ in $\mathbb{Q}[x]$ of degree 5 can be solved by radicals if and only if its Galois group (considered as a subgroup of S_5) is contained in the Frobenius group of order 20. It is known that this is the case if and only if an associated polynomial $g(x)$ of degree 6 has a rational root (cf. Dummit, *Solving Solvable Quintics*, Math. Comp., 57(1991), pp. 387–401). If the quintic is in the general form (where a translation is performed so that the coefficient of x^4 is zero)

$$f(x) = x^5 + px^3 + qx^2 + rx + s \qquad p, q, r, s \in \mathbb{Q}$$

then the associated polynomial of degree 6 is

$$\begin{aligned} g(x) = x^6 &+ 8rx^5 + (2pq^2 - 6p^2r + 40r^2 - 50qs)\, x^4 \\ &+ (-2q^4 + 21pq^2r - 40p^2r^2 + 160r^3 - 15p^2qs - 400qrs + 125ps^2)\, x^3 \\ &+ (p^2q^4 - 8q^4r + 9p^4r^2 - 136p^2r^3 + 625q^2s^2 + 400r^4 - 6p^3q^2r \\ &\quad + 76pq^2r^2 - 50pq^3s - 1400qr^2s + 500prs^2 + 90p^2qrs)\, x^2 \\ &+ (-108p^5s^2 + 32p^4r^3 - 256p^2r^4 - 3125s^4 + 512r^5 - 2pq^6 + 3q^4r^2 \\ &\quad - 58q^5s + 2750q^2rs^2 - 31p^3q^3s - 500pr^2s^2 + 19p^2q^4r \\ &\quad - 51p^3q^2r^2 + 76pq^2r^3 - 2400qr^3s - 325p^2q^2s^2 + 525p^3rs^2 \\ &\quad + 625pqs^3 + 117p^4qrs + 105pq^3rs + 260p^2qr^2s)\, x \\ &+ (q^8 + 256r^6 + 17q^4r^3 - 27p^7s^2 - 4p^6r^3 + 48p^4r^4 - 192p^2r^5 \\ &\quad + 3125p^2s^4 - 9375rs^4 - 1600qr^4s - 99p^5rs^2 - 125pq^4s^2 \\ &\quad - 124q^5rs + 3250q^2r^2s^2 - 2000pr^3s^2 - 13pq^6r + p^5q^2r^2 \\ &\quad + 65p^2q^4r^2 - 128p^3q^2r^3 - 16pq^2r^4 - 4p^5q^3s - 12p^2q^5s \\ &\quad - 150p^4q^2s^2 + 1200p^3r^2s^2 + 18p^6qrs + 12p^3q^3rs + 196p^4qr^2s \\ &\quad + 590pq^3r^2s - 160p^2qr^3s - 725p^2q^2rs^2 - 1250pqrs^3). \end{aligned}$$

In the particular case where $f(x) = x^5 + Ax + B$ this polynomial is simply

$$g(x) = x^6 + 8Ax^5 + 40A^2x^4 + 160A^3x^3 + 400A^4x^2 + (512A^5 - 3125B^4)x - 9375AB^4 + 256A^6.$$

(a) Use this criterion to prove that the Galois group over $\mathbb{Q}$ of the polynomial $x^5 - 5x + 12$ is the dihedral group of order 10. [Show the associated sixth degree polynomial is

$$x^6 - 40x^5 + 1000x^4 - 20000x^3 + 250000x^2 - 66400000x + 976000000$$

and has $x = 40$ as a rational root. Cf. also Exercise 35 in Section 6.]

(b) Use this criterion to prove that $x^5 - x - 1$ is not solvable by radicals.