Note: you can use the Eisenstein criterion for irreducibility of polynomials over $\mathbb{Q}$ if need be.

(1) An unsolved problem asks whether for an arbitrary finite group $G$ there exists a Galois extension $\mathbb{Q} \subseteq L$ whose Galois group is isomorphic to $G$. We want to show that this holds for abelian groups.

(i) Let $p$ be an odd prime. Show that for every $n \geq 2$, $(1+p)p^{n-2} \equiv 1+p^{n-1} \pmod{p^n}$. Deduce that $1+p$ has order $p^{n-1}$ in $(\mathbb{Z}/\langle p^n \rangle)^*$. 

(ii) If $b \in \mathbb{Z}$ with $(p,b) = 1$ and $b$ has order $p-1$ in $(\mathbb{Z}/\langle p \rangle)^*$ and $n \geq 1$, show that $b^{p-1}$ has order $p-1$ in $(\mathbb{Z}/\langle p^n \rangle)^*$. Deduce that for $n \geq 1$, $(\mathbb{Z}/\langle p^n \rangle)^*$ is cyclic.

(iii) Show that for every $n \geq 3$, we have $5^{2^{n-3}} \equiv 1+2^{n-1} \pmod{2^n}$. Deduce that $(\mathbb{Z}/\langle 2^n \rangle)^*$ is generated by the classes of 5 and $-1$, and is isomorphic to $(\mathbb{Z}/\langle 2^n-2 \rangle) \times (\mathbb{Z}/\langle 2 \rangle)$ for any $n \geq 2$.

(iv) Use the Chinese Remainder Theorem to deduce the structure of $(\mathbb{Z}/\langle m \rangle)^*$ in general.

(v) Dirichlet’s theorem on primes in arithmetic progressions states that if $a$ and $b$ are coprime positive integers, then the set $\{an+b|n \in \mathbb{N}\}$ contains infinitely many primes. Use this, the structure theorem for finite abelian groups, and part (iv) to show that every finite abelian group is isomorphic to a quotient of $(\mathbb{Z}/\langle m \rangle)^*$ for suitable $m$. Deduce that every finite abelian group is the Galois group of some Galois extension $\mathbb{Q} \subseteq L$.

(2) Let $K$ be a field containing an $n$-th primitive root of unity for some $n \geq 1$. Let $a, b \in K$ such that the polynomials $f(t) = t^n - a$ and $g(t) = t^n - b$ are irreducible. Show that $f$ and $g$ have the same splitting field if and only if $b = c^n a^r$ for some $c \in K$ and $r \in \mathbb{N}$ with $\gcd(r,n) = 1$.

(3) Let $p$ be a prime, $K$ be a field with $\text{char } K \neq p$, and $L$ the $p$-th cyclotomic extension of $K$. For $a \in K$, show that $t^p - a$ is irreducible over $K$ if and only if it is irreducible over $L$. Is the result true if $p$ is not assumed to be prime?

(4) Let $K$ be a field containing an $n$-th primitive root of unity. Show that $t^n - a$ is reducible over $K$ if and only if $a$ is a $d$-th power in $K$ for some divisor $d > 1$ of $n$. Show that this need not be true if $K$ does not contain an $n$-th primitive root of unity.

(5) Let $K \subseteq L$ be a field extension of degree 2 and assume $\text{char } K \neq 2$. Show that the extension is a Kummer extension.

(6) Let $K$ be a field of char $K = 0$ and $L$ the $n$-th cyclotomic extension of $K$. Show that there is a sequence of Kummer extensions $E_0 = K \subseteq E_1 \subseteq \cdots \subseteq E_r$ such that $L$ is contained in $E_r$. (Hint: consider $F = \text{splitting field of}$
\((t^n - 1)(t^{n-1} - 1) \cdots (t - 1)\) and apply induction on \(n\)

(7) Let \(F, E\) be intermediate fields of a finite separable extension \(K \subseteq L\). Show that if \(K \subseteq F\) and \(K \subseteq E\) are solvable extensions, then \(K \subseteq FE\) is also solvable. Here \(FE\) is the composite field of \(F\) and \(E\), i.e., the intermediate field generated by the elements of \(F, E\) (that is, the set of all finite sums \(\sum x_i y_i \) for \(x_i \in F, y_i \in E\)).

(8) Write \(\cos(2\pi/17)\) explicitly in terms of radicals.

(9) Let \(K\) be a field, \(f \in K[t]\) be separable, and \(L\) be the splitting field of \(f\) over \(K\). Show that \(f\) is irreducible iff \(\text{Gal}(L/K)\) acts transitively on \(\text{Root} f(L)\) (that is, for any two roots \(\alpha, \beta\) there is \(\varphi \in \text{Gal}(L/K)\) such that \(\varphi(\alpha) = \beta\)).

(10) Let \(f\) be an irreducible cubic polynomial over a field \(K\) with \(\text{char } K \neq 2\), and let \(\alpha\) be a square root of the discriminant of \(f\). Show that \(f\) remains irreducible over \(K(\alpha)\).

(11) Let \(f\) be an irreducible quartic polynomial over a field \(K\) with \(\text{char } K \neq 2\) and let \(L\) be its splitting field over \(K\). Assume that the Galois group of \(K \subseteq L\) is isomorphic to \(A_4\). Show that \(L\) can be written in the form \(F(\sqrt{a}, \sqrt{b})\) where \(K \subseteq F\) is a Galois extension of degree 3 and \(a, b \in F\).

(12) Consider the quartic \(f = t^4 - 4t + 2\) and let \(L\) be its splitting field over \(\mathbb{Q}(\sqrt{-1})\). Find the Galois group \(\text{Gal}(L/\mathbb{Q}(\sqrt{-1}))\).

(13) **Ruler-compass constructions.** We will apply Galois theory to an ancient question which asks whether the side of a cube of volume 2 can be constructed by ruler-compass constructions. Consider the Euclidean plane \(\mathbb{R}^2\). For a finite subset \(S \subseteq \mathbb{R}^2\) we have two constructions. First we have ruler: given \(P, Q \in S\), we can join them by a straight line. Second we have compass: given points \(P, Q, Q' \in S\), we can draw a circle with centre \(P\) and radius equal to \(QQ'\). We say that a point \(R\) in the plane is 1-step constructible from \(S\) if \(R\) is a point of intersection of 2 distinct curves (lines or circles) obtained from \(S\) by either of the above two constructions. A point \(R\) is constructible from \(S\) if there exist points \(R_1, \ldots, R_n = R\) such that \(R_1\) is 1-step constructible from \(S\), and for each \(1 \leq i \leq n - 1\), \(R_{i+1}\) is 1-step constructible from \(S \cup \{R_1, \ldots, R_i\}\). A set \(T\) constructible from \(S\) is similarly defined.

We define the field \(\mathbb{Q}(S)\) to be the field generated over \(\mathbb{Q}\) by the coordinates of all the points of \(S\).

(i) Show that if \(R\) is 1-step constructible from \(S\) then \([\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = 1\) or 2.

(ii) Show that if a set \(T\) is constructible from \(S\) then \([\mathbb{Q}(T) : \mathbb{Q}(S)]\) is a power of 2.

(iii) Assume \(\mathbb{Q}(S) = \mathbb{Q}\). Show that \((0, \sqrt[3]{2})\) is not constructible from \(S\). (This answers the ancient question negatively)