Computations of Galois groups

$x^3 - 3x + 17 \in \mathbb{Q}[x]$.  

An easy check using the rational zeros theorem shows that this polynomial has no rational roots, so it's irreducible. Its discriminant is

$$D = -4(-3)^3 - 27(17)^2 = -7695.$$  

So the polynomial has exactly one real root and

$$\text{Gal}(x^3 - 3x + 17) \cong S_3.$$  

$x^{10} + x^5 + 1 \in \mathbb{Q}[x]$  

This polynomial may be written as $(x^5)^2 + (x^5) + 1$. The roots of $y^2 + y + 1$ are cube roots of unity; indeed,

$$(y^2 + y + 1)(y - 1) = y^3 - 1.$$  

So $y = e^{2\pi i/3}$, $e^{-2\pi i/3}$ are its roots. It is immediate that the roots of $x^{10} + x^5 + 1$ are fifteenth roots of unity, and that the primitive fifteenth root of unity $e^{2\pi i/15}$ is a root of this polynomial. So $\mathbb{Q}(e^{2\pi i/15})$ is a splitting field of the polynomial over $\mathbb{Q}$. 
Now \( \text{Gal}(\mathbb{Q}(e^{2\pi i/15})/\mathbb{Q}) \cong \left( \mathbb{Z}/15\mathbb{Z} \right)^{\times} \),

\[
\cong \{1, 2, 4, 7, 8, 11, 13, 14\} \quad \text{(under the operation of multiplication)}.
\]

This is an abelian group of order 8, and is in fact isomorphic to \( \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \), via

\[
\psi: \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow (\mathbb{Z}/15\mathbb{Z})^{\times}
\]

\[
\psi(a/b) = 2^a(11)^b.
\]

\[x^4 - 5 \text{ over } \mathbb{Q} \text{ and } \mathbb{Q}(\sqrt{5})\]

Let \( \sqrt[4]{5} \) be a positive real 4th root of 5.

Then \( \sqrt[4]{5}, i\sqrt[4]{5}, -\sqrt[4]{5}, -i\sqrt[4]{5} \) give the four distinct roots of \( x^4 - 5 \). It's immediate that \( \mathbb{Q}(\sqrt[4]{5}, i) \) is a splitting field over \( \mathbb{Q} \).

Consider \( \mathbb{Q} \leq \mathbb{Q}(\sqrt{5}) \leq \mathbb{Q}(\sqrt[4]{5}, i) \).

Then \( \mathbb{Q}(\sqrt{5})/\mathbb{Q} \) is a splitting field of \( x^2 - 5 \), so its Galois group is \( \mathbb{Z}/2\mathbb{Z} \). Over \( \mathbb{Q}(\sqrt{5}) \), the extension \( \mathbb{Q}(\sqrt[4]{5}, i) \) is a splitting field of \( (x^2 - \sqrt{5})(x^2 + \sqrt{5}) = x^4 - 5 \).

There are two subfields \( \mathbb{Q}(\sqrt[4]{5}), \mathbb{Q}(i\sqrt[4]{5}) \) corresponding to the two quadratics; their intersection is \( \mathbb{Q}(\sqrt{5}) \).
so \( \text{Gal} \left( \mathbb{Q} \left( \sqrt[5]{5}, i \right) / \mathbb{Q} \left( \sqrt[5]{5} \right) \right) \cong (\mathbb{Z}/2\mathbb{Z})^2 \). It's then immediate that \( |\text{Gal} \left( \mathbb{Q} \left( \sqrt[5]{5}, i \right) / \mathbb{Q} \right)| = 8 \), so \( \text{Gal} \left( \mathbb{Q} \left( \sqrt[5]{5}, i \right) / \mathbb{Q} \right) \cong D_4 \).

\[
x^3 - 12x + 21 \quad \text{over } \mathbb{Q}, \mathbb{R}
\]

The discriminant is

\[
D = -4(-12)^3 - 27(21)^2 = 6912 - 11907 = -4995.
\]

A quick check using the rational zeroes theorem shows that none of the divisors of 21 is a root, so the polynomial has no rational roots. Hence the polynomial has exactly one real root and its Galois group over \( \mathbb{Q} \) is \( S_3 \). Over \( \mathbb{R} \), it splits as a linear term times an irreducible quadratic; hence its Galois group over \( \mathbb{R} \) is \( \mathbb{Z}/2\mathbb{Z} \).

\[
x^4 - x^2 - 6 \quad \text{over } \mathbb{Q}.
\]

This polynomial may be written

\[
(x^2)^2 + (x^2) - 6.
\]

The quadratic formula shows that \( y^2 + y - 6 \) has roots 2, -3. So \( x^4 + x^2 - 6 \) has roots \( \pm i\sqrt{3}, \pm \sqrt{2} \); and \( x^4 + x^2 - 6 = (x^2 - 2)(x^2 + 3) \).
Then \( \mathbb{Q}(\sqrt[4]{2}, i\sqrt[3]{3}) \) is a splitting field of \( x^4 + x^2 - 6 \) over \( \mathbb{Q} \). Since \( \mathbb{Q}(\sqrt[4]{2}) \cap \mathbb{Q}(i\sqrt[3]{3}) = \mathbb{Q} \), we find that
\[
\text{Gal}(x^4 + x^2 - 6) \cong \mathbb{Z}/2 \times \mathbb{Z}/2,
\]
over \( \mathbb{Q} \).

\[ x^4 + x^2 + x + 1 \]

It follows from the rational zeros theorem and a computation that this polynomial has no rational roots. Since its content is a unit, it is irreducible over \( \mathbb{Q} \) iff it is irreducible over \( \mathbb{Z} \).

Suppose
\[ x^4 + x^2 + x + 1 = (x^2 + ax + b)(x^2 - ax + c), \text{ in } \mathbb{Z}[x]. \]

Then \( bc = 1 \), so \( b = c = \pm 1 \). Also
\[ a(c-b) = 1, \text{ a contradiction. So } x^4 + x^2 + x + 1 \]
is irreducible.

Its resolvent cubic is
\[ g(x) = x^3 - 2x^2 - 3x + 1. \]

It's easily checked to have no roots in \( \mathbb{Q} \).

The associated reduced cubic is \( \tilde{g}(x) = g(x + \frac{2}{3}) \), which I compute to be
\[ \tilde{g}(x) = x^3 - \frac{13}{3}x - \frac{43}{27}. \]

\* I.e. it is primitive!
The discriminant of \( \tilde{\alpha} \) is
\[
D = -4 \left( -\frac{13}{3} \right)^3 - 27 \left( -\frac{13}{27} \right)^2
\]
\[
= \frac{8788}{27} - \frac{1849}{27} = \frac{6941}{27}
\]

Now \( \sqrt[3]{D} \notin \mathbb{Q} \), so \( \text{Gal}(\tilde{\alpha}) \cong \text{Gal}(x^3) \cong S_3 \).

It follows that \( \text{Gal}(x^4 + x^2 + x + 1) = S_4 \).

Which of \( x^5 - 3x^2 + 2 \), \( x^5 - 13x + 13 \), \( x^5 - 4x - 2 \) are solvable by radicals over \( \mathbb{Q} \)?

The first polynomial has 1 as a root, so its Galois group is the same as the Galois group of the quartic \( \frac{x^5 - 3x^2 + 2}{x - 1} \). (which is a polynomial), hence a subgroup of \( S_4 \), hence solvable, so \( x^5 - 3x^2 + 2 \) is solvable by radicals. By Eisenstein's Criterion, \( x^5 - 13x + 13 \) and \( x^5 - 4x - 2 \) are irreducible over \( \mathbb{Q} \). Calculus easily shows that both have exactly 3 real roots, so, by the same argument we used in class, their Galois groups are \( S_5 \) and the polynomials are not solvable by radicals.
\[4x^4 + 12x + 9 \text{ over } \mathbb{Q}\] This is irreducible by Eisenstein.

Replacing it by \[x^4 + \frac{12}{4}x + \frac{9}{4} = x^4 + 3x + \frac{9}{4},\] its resolvent cubic is

\[g(x) = x^3 - 9x + 9.\]

One easily checks that \(\pm 1, \pm 3, \pm 9\) are not roots of \(g\), so by the rational zeros theorem \(g\) has no roots in \(\mathbb{Q}\), hence is irreducible. Its discriminant is

\[\Delta = -4(-9)^3 - 27(9)^2 = 2916 - 2187 = 729 = (27)^2.\]

So \(\text{Gal}(g) \cong \mathbb{Z}/3\mathbb{Z}\), and \(\text{Gal}(4x^4 + 12x + 9) \cong A_4\).

Now, \(A_4\) has no subgroups of order 6: if it had one, it would be normal in \(A_4\) since it would be of index 2. Such a subgroup \(M\), however, would contain an element of order 2; after re-indexing, we might assume \((12)(34) \in M\). Then

\[(123)^{-1}(12)(34)(123) = (13)(24).\]

It follows that, since \(M\) is normal,

\[H = \langle (1), (12)(34), (13)(24), (14)(23) \rangle \leq M,\]

contradicting \(|M| = 6\).

Let \(E\) be a splitting field of \(4x^4 + 12x + 9\) over \(\mathbb{Q}\), let \(\mathbb{Q} \subseteq K \subseteq E\) be an intermediate field given by \(K = E^{(123)}\).\]
By the Fundamental Theorem of Galois Theory,
\[ [K : \mathbb{Q}] = [\mathbb{A}_4 : \langle (123) \rangle] = 4. \]
But the Fundamental Theorem implies, since \( A_4 \) has no subgroups of index 2, that there are no intermediate extensions \( \mathbb{Q} \leq L \leq K \) with
\[ [L : \mathbb{Q}] = 2. \]
Consider the extension $F_p(x, y)$ of $F_p(x^p, y^p)$. We have $F_p(x^p, y^p)(x, y) = F_p(x, y)$; the elements $x, y \in F_p(x, y)$ are algebraic over $F_p(x^p, y^p)$, so $F_p(x, y)/F_p(x^p, y^p)$ is a finitely generated algebraic extension, hence is finite.

Given $\frac{f}{g} \in F_p(x, y)/F_p(x^p, y^p)$, consider $h(z) = z^p + \left(\frac{f}{g}\right)^p$. We have

$$\frac{f(x, y)^p}{g(x, y)^p} = \frac{f(x^p, y^p)}{g(x^p, y^p)}$$ since $c^p = c$ for all $c \in F_p$.

So $h \in F_p(x^p, y^p)[z]$. Over $F_p(x, y)$, we find that $h$ factors as $h(z) = (z + \frac{f}{g})^p$. It is easy to check that $h$ is irreducible in $F_p(x^p, y^p)[z]$. Hence $F_p(x^p, y^p)(\frac{f}{g}) \subseteq F_p(x, y)$ satisfies $F_p(x^p, y^p)(\frac{f}{g}) = F_p(x^p, y^p)[z]/(h)$.

It follows that if $F_p(x, y)$ were a simple extension of $F_p(x^p, y^p)$, then $[F_p(x, y) : F_p(x^p, y^p)] = p$. 

On the other hand, we have an intermediate extension

\[ F_p(x^p, y^p) \subset F_p(x^p, y^p)(x) = F_p(x^p, y^p) \subset F_p(x^p, y^p)(y) = F_p(x^p, y^p). \]

We find that

\[ [F_p(x, y) : F_p(x, y^p)] = [F_p(x, y) : F_p(x, y^p)] [F_p(x, y^p) : F_p(x^p, y^p)] \]

\[ = p \cdot p = p^2; \] indeed, each of the intermediate extensions is nontrivial and is a splitting field of a purely inseparable polynomial \((x^p + y^p) \text{ or } (x^p + y^p)\) of degree \(p\), so it follows that each has degree \(p\).

Thus \( F_p(x, y) \) is not a simple extension of \( F_p(x^p, y^p) \).

One can find infinitely many intermediate extensions between \( F_p(x^p, y^p) \) and \( F_p(x, y) \) as follows.

Given \( f \in F_p(x, y) \setminus F_p(x^p, y^p) \),

\( F_p(x^p, y^p)(f) \) is the span of \( 1, f, f^2, \ldots, f^{p-1} \) in \( F_p(x, y) \) as an \( F_p(x^p, y^p) \)-vector space; this is a \( p \)-dimensional subspace of the \( p^2 \)-dimensional space \( F_p(x, y) \). Our base field \( F_p(x^p, y^p) \) is infinite, so if \( V_1, \ldots, V_k \in F_p(x, y) \) is any finite
list of $p$-dimensional subspaces, the set
$$F_p(x, y) \setminus \left( \bigcup_{i=1}^k V_i \right)$$
is nonempty.

Suppose $F_p(x^p, y^p) \subset V_i \subset F_p(x, y)$ is an intermediate field of degree $p$ over $F_p(x^p, y^p)$. If $f \in F_p(x, y) \setminus V_i$ then $F_p(x^p, y^p)(f)$ is an intermediate extension between $F_p(x^p, y^p)$ and $F_p(x, y)$ of degree $p$ over $F_p(x^p, y^p)$. Since $f \notin V_i$, $F_p(x^p, y^p)(f) \neq V_i$.

So, choose $f_i \in F_p(x, y) \setminus F_p(x^p, y^p)$, and let $V_i = F_p(x^p, y^p)(f_i)$. Given fields $F_p(x^p, y^p) \subset V_i \subset F_p(x, y)$ with $[V_i : F_p(x^p, y^p)] = p, \ i = 1, \ldots, k$, choose $f_{k+i} \in F_p(x, y) \setminus \left( \bigcup_{i=1}^k V_i \right)$, and let $V_{k+i} = F_p(x^p, y^p)(f_i)$. Then $V_1, V_2, \ldots$ is an infinite list of pairwise distinct intermediate extensions between $F_p(x^p, y^p)$ and $F_p(x, y)$. 
