Problem 1. *Give an example of fields $F \subset E \subset K$ such that K is a root extension of F but E is not a root extension of F. (Hint: Look at $K = \mathbb{Q}(\zeta)$ where ζ is the primitive 7th root of unity).*

For the rest of the problem we will use ζ to refer to the primitive 7th root of unity. Begin with the field extension $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. The minimal polynomial is the cyclotomic Φ_7. We know that the Galois group of Φ_7, and thus $\mathbb{Q}(\zeta)$, is

$$\mathrm{Gal}(\mathbb{Q}(\zeta)) \cong \mathbb{Z}_7^*$$

where the automorphisms contained within are of the form

$$\sigma_n(\zeta^i) = \zeta^{ni}$$

Note that there is a subgroup of order 2 generated by σ_6 since $6^2 \equiv 1 \mod 7$. From the Fundamental Theorem of Galois theory there is a field extension of $\mathbb{Q}$ corresponding to this subgroup. One of the elements fixed by this subgroup is $\zeta + \zeta^6$ as $\sigma_6(\zeta + \zeta^6) = \zeta^6 + \zeta^{36} = \zeta^6 + \zeta$.

The minimal polynomial for the element $\zeta + \zeta^6$ is $x^3 + x^2 - 2x - 1$. The other roots are of the form $(\zeta + \zeta^6)^2 - 2$ and $-(\zeta + \zeta^6)^2 - (\zeta + \zeta^6) + 1$. Moreover all of these roots are real: $2\cos(\frac{2\pi}{7}), -2\cos(\frac{3\pi}{7})$, and $2\cos(\frac{3\pi}{7}) - 2\cos(\frac{2\pi}{7}) - 1$ respectively.

Thus $\mathbb{Q}(\zeta + \zeta^6)$ is the splitting field for $x^3 + x^2 - 2x - 1$. However the extension does not tread into the complex numbers while each of the roots had to be constructed from sums of complex numbers. Therefore the field $\mathbb{Q}(\zeta + \zeta^6)$ is not a root extension of $\mathbb{Q}$ even though $\mathbb{Q}(\zeta)$ is.

Problem 2. *Let $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{3})$, $K = \mathbb{Q}(\sqrt{\sqrt{3}+1})$. Show that E/F and K/E are Galois extensions, but that K/F is not Galois. Find the minimal polynomial of $\sqrt{\sqrt{3}+1}$ and find its Galois group.*

We can see that E/F and K/E are Galois since they are both splitting fields of separable polynomials $x^2 - 3$ and $x^2 - (\sqrt{3} + 1)$ respectively.

Now we will show that the K/F is not Galois. First note that the minimal polynomial of $\sqrt{\sqrt{3}+1}$ is $x^4 - 2x^2 - 2$. If it was Galois then it would contain all of the roots which are $\pm\sqrt{1 \pm \sqrt{3}}$. However then it would contain the product

$$\sqrt{1+\sqrt{3}}\sqrt{1-\sqrt{3}} = i\sqrt{2}$$

However $i \notin K$ which shows that K/E is not Galois.

To find the Galois group of $f(x) = x^4 - 2x^2 - 2$ we will follow the procedure in Dummit and Foote beginning on page 615. The resolvent cubic for f is $h(x) = x^3 + 4x^2 + 12x$. Since h is reducible into a linear term and a quadratic the Galois group is either $\mathbb{Z}_4$ or D_8. However since the discriminant of f is -4608 which is negative. As such the Galois group cannot be cyclic. Therefore $\mathrm{Gal}(x^4 - 2x^2 - 2) \cong D_8$.

Problem 3. *Find a root extension of $\mathbb{Q}$ containing the splitting fields of each of the following polynomials.*

(a) $x^4 + 1$

(b) $x^4 + 3x^2 + 1$

(c) $x^5 + 4x^3 + x$

(d) $(x^3 - 2)(x^7 - 5)$

(a) The roots of x^4+1 are $e^{\pi i/4}, e^{3\pi i/4}, e^{5\pi i/4}$, and $e^{7\pi i/4}$. Since these are all roots of $x^4-(-1)$ the field $\mathbb{Q}[e^{\pi i/4}, e^{3\pi i/4}, e^{5\pi i/4}, e^{7\pi i/4}]$ has a root tower from adjoining each one in turn.

(b) The roots of x^4+3x^2+1 are $\pm\sqrt{\frac{-3\pm\sqrt{5}}{2}}$. The splitting field will then be contained in the root tower where we adjoint $\sqrt{5}$ followed by $\sqrt{3+\sqrt{5}}$ and finally i.

(c) The roots of x^5+4x^3+x are $0, \pm\sqrt{-2\pm\sqrt{3}}$. Similar to part (b) we can get a root tower containing the splitting field by adjoining $\sqrt{3}$, $\sqrt{2+\sqrt{3}}$, and i in order.

(d) The roots of $(x^3-2)(x^7-5)$ are $\sqrt{2}\zeta_3^i, \sqrt{5}\zeta_7^j$ for $0 \leq i < 3$ and $0 \leq j < 7$. We can then obtain a root extension containing the splitting field by adjoining each of the roots in turn.

Problem 4. *Give an example of a polynomial $\mathbb{Q}[x]$ which is solvable by radicals, but whose splitting field is not a root extension of $\mathbb{Q}$.*

Using the example from problem 1 we have that the polynomial $f(x) = x^3+x^2-2x-1$. We will show that is it solvable by calculating its Galois group explicitly from the procedure outlined in Dummit and Foote pg 612. First note that f is irreducible. Thus its Galois group is either S^3 or A_3. However since the discriminant of f is square $(49 = 7^2)$ we have that the Galois group is A_3 which is indeed a solvable group.

Thus f is solvable by radicals as $\mathrm{Gal}(\mathbb{Q}(\zeta_7+\zeta_7^6)) \cong \mathrm{Gal}(f)$ is isomorphic to A_3 which is solvable. However it is not a root extension of $\mathbb{Q}$.

Problem 5. *For r a positive integer, define $f_r(x) \in \mathbb{Q}[x]$ by*

$$f_r(x) = (x^2+4)x(x^2-4)(x^2-16)\cdots(x^2-4r^2)$$

(a) Give a (rough) sketch of the graph of $f_r(x)$

(b) Show that if k is an odd integer, then $|f_r(k)| \geq 5$.

(c) Show that $g_r(x) = f_r(x)-2$ is irreducible over $\mathbb{Q}$ and determine its Galois group when $2r+3 = p$ is prime.

Proof. (a) Will have roots at $\pm 2r$ then go off on its own.

(b)

(c) First note that for $f_r(x)$ is monic and that the coefficient for every other term will be divisible by 2 as $4r^2$ is even. Moreover as we multiply by x in the product form the polynomial has no constant term. Thus $g_r(x) = f_r(x)-2$ is irreducible by Eisenstein's criterion with 2.

Since $|f_r(k)| \geq 5$ for odd k we know that g_r will have the same number of roots as f_r. We also know that there are two complex roots. As such one of the automorphisms in our Galois group will be a transposition supplied by complex conjugation. In addition since g_r is irreducible the action of the Galois group on the roots is transitive. Since the degree of g_r is prime we have that $\mathrm{Gal}(g_r) \cong S_p$ as the group is transitive and contains a transposition.

□