Cavallaro, Jeffery
Math 221b
Homework #7

1). Suppose we have an extension of fields $F \subseteq E \subseteq L \subseteq K$ and let $G = \mathrm{Aut}(K/F)$ with subgroups $I \leq J \leq H \leq G$.

a). Show that $G = \mathrm{Aut}(K/F)$ is actually a group under composition of functions.

Assume $\varphi_1, \varphi_2 \in G$ and $\alpha \in F$.
By definition, φ_1 and φ_2 fix F, so $\varphi_1(\alpha) = \alpha$ and $\varphi_2(\alpha) = \alpha$.

$$(\varphi_1\varphi_2)(\alpha) = \varphi_1(\varphi_2(\alpha)) = \varphi_1(\alpha) = \alpha$$

Thus, $\varphi_1\varphi_2$ fixes F and so $\varphi_1\varphi_2 \in G$.

Therefore G is closed under the operation.

Function composition is associative.

Assume $\varphi \in G$ and $\alpha \in F$:

$$\iota_K(\alpha) = \alpha$$

Thus i_K fixes F and so $\iota_K \in G$. But also:

$$\iota_k\varphi = \varphi\iota_k = \varphi$$

Therefore G has identity ι_K.

Assume $\varphi \in G$ and $\alpha \in F$.
By definition, φ fixes F, so $\varphi(\alpha) = \alpha$.
But φ is bijective, so φ^{-1} exists and:

$$\varphi^{-1}(\alpha) = \varphi^{-1}(\varphi(\alpha)) = (\varphi^{-1}\varphi)(\alpha) = \iota_K(\alpha) = \alpha$$

Thus, φ^{-1} fixes F and so $\varphi^{-1} \in G$.

Therefore G is closed under inverses.

Therefore G is a group under the operation of function composition.

b). Show that $G(L)$ is actually a subgroup of G.

Assume $\alpha \in L$.

$$\iota_L(\alpha) = \alpha$$

Thus ι_L fixes L and so $\iota_L \in G(L)$.

$\therefore G(L) \neq \emptyset$

Assume $\varphi \in G(L)$ and $\alpha \in F$.
But since $F \subseteq L$ we have $\alpha \in L$ also and since φ fixes L:

$$\varphi(\alpha) = \alpha$$

Thus, φ fixes F and so $\varphi \in G$.

$\therefore G(L) \subseteq G$

Assume $\varphi_1, \varphi_2 \in G(L)$ and assume $\alpha \in L$.
By definition, φ_1 and φ_2 fix L, so $\varphi_1(\alpha) = \alpha$ and $\varphi_2(\alpha) = \alpha$.
Also, φ_2 is bijective so φ_2^{-1} exists.

$$\begin{aligned}(\varphi_1\varphi_2^{-1})(\alpha) &= \varphi_1(\varphi_2^{-1}(\alpha)) \\ &= \varphi_1(\varphi_2^{-1}(\varphi_2(\alpha))) \\ &= \varphi_1((\varphi_2^{-1}\varphi_2)(\alpha))) \\ &= \varphi_1(\iota_L(\alpha)) \\ &= \varphi_1(\alpha) \\ &= \alpha\end{aligned}$$

Thus $\varphi_1\varphi^{-1}$ fixes L and so $\varphi_1\varphi^{-1} \in G(L)$.

Therefore, by the subgroup test, $G(L) \leq G(F)$.

c). Prove the inclusions $G(L) \leq G(E)$ and $F(H) \subseteq F(J)$

From the previous problem we already know that $G(L), G(E) \leq G$, and so it suffices to show inclusion:

Assume $\varphi \in G(L)$

$\forall\, \alpha \in L, \varphi(\alpha) = \alpha$
Since $E \subseteq L, \forall\, \alpha \in E, \varphi(\alpha) = \alpha$
$\varphi \in G(E)$

$\therefore G(L) \leq G(E)$

Assume $\alpha \in F(H)$

$\forall\, \varphi \in H, \varphi(\alpha) = \alpha$
Since $J \subseteq H, \forall\, \varphi \in J, \varphi(\alpha) = \alpha$
So $\alpha \in F(J)$

$\therefore F(H) \subseteq F(J)$

d). Prove the inclusions $H \leq G(F(H))$ and $L \subseteq F(G(L))$

From the previous problem we already know that $H, G(F(H)) \leq G$, and so it suffices to show inclusion:

Assume $\varphi \in H$.
By definition, φ fixes everything in $F(H)$.
So, by definition, $\varphi \in G(F(H))$.

$\therefore H \leq G(F(H))$

Now, assume $\alpha \in L$.
By definition, α is fixed by everything in $G(L)$.
So, by definition, $\alpha \in F(G(L))$.

$\therefore L \subseteq F(G(L))$

e). Prove that $G(L)$ and $F(H)$ are closed.

From (d), we already know that $G(L) \subseteq G(F(G(L)))$.

Assume $\varphi \in G(F(G(L)))$.
φ fixes everything in $F(G(L))$.
But also from (d), $L \subseteq F(G(L))$.
So φ fixes everything in L.
Thus, by definition, $\varphi \in G(L)$.

$\therefore G(L) = G(F(G(L)))$ and so $G(L)$ is closed.

From (d), we already know that $F(H) \subseteq F(G(F(H)))$.

Assume $\alpha \in F(G(F(H)))$.
α is fixed by everything in $G(F(H))$.
But also from (d), $H \subseteq G(F(H))$.
So α is fixed by everything in H.
Thus, by definition, $\alpha \in F(H)$.

$\therefore F(H) = F(G(F(H)))$ and so $F(H)$ is closed.

2). Suppose we have an extension of fields $F \subseteq L \subseteq K$ and let $G = \mathrm{Aut}(K/F)$ with subgroups $1 \leq H \leq G$:

a). Show that L is stable $\implies G(L) \trianglelefteq G$

Assume L is stable.

Assume $\varphi \in G(L)$.
Assume $\alpha \in L$.
φ fixes L and so $\varphi(\alpha) = \alpha$.

Now, assume $\psi \in G$.
Since ψ is bijective and L is stable, $\exists\, \beta \in L$ such that $\psi(\beta) = \alpha$ and $\psi^{-1}(\alpha) = \beta$.
Also, since $\beta \in L$, φ also fixes β and so $\varphi(\beta) = \beta$

$(\psi\varphi\psi^{-1})(\alpha) = \psi(\varphi(\psi^{-1}(\alpha))) = \psi(\varphi(\beta)) = \psi(\beta) = \alpha$
Thus, $\psi\varphi\psi^{-1} \in G(L)$.

$\therefore G(L) \trianglelefteq G$.

b). Show that $H \trianglelefteq G \implies F(H)$ is stable.

Assume $H \trianglelefteq G$.

Assume $\varphi \in H$.
Assume $\psi \in G$.
Since $H \trianglelefteq G$, we have $\psi^{-1}\varphi\psi \in H$.

Now, assume $\alpha \in F(H)$
α is fixed by H and $\psi^{-1}\varphi\psi \in H$, so $(\psi^{-1}\varphi\psi)(\alpha) = \alpha$.
$(\varphi\psi)(\alpha) = \psi(\alpha)$
$\varphi(\psi(\alpha)) = \psi(\alpha)$
So $\psi(\alpha)$ is fixed by φ and thus $\psi(\alpha) \in F(H)$.

Therefore $F(H)$ is stable.

3). Suppose $K/\mathbb{Q}$ is a quadratic extension ($[K : \mathbb{Q}] = 2$):

a). Show that $K = \mathbb{Q}(\sqrt{d})$ for some squarefree integer $d \neq 1$.

b). Show that $K/\mathbb{Q}$ is Galois with $\mathrm{Gal}(K/Q) \cong \mathbb{Z}/2\mathbb{Z}$.

Assume $\alpha \in K$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. The minimum polynomial is given by:

$$m_{\alpha,\mathbb{Q}}(x) = x^2 + bx + c$$

for some $b, c \in \mathbb{Q}$. The roots for this polynomial are found as follows:

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

If $\sqrt{b^2 - 4c} \in \mathbb{Q}$ then $[K : \mathbb{Q}] = 1$, so assume not.
Let $b = \frac{p}{q}$ and $c = \frac{h}{k}$ where $p, q, h, k \in \mathbb{Z}$ and $q, k \neq 0$:

$$\begin{aligned} x &= \frac{-\frac{p}{q} \pm \sqrt{\left(\frac{p}{q}\right)^2 - \frac{4h}{k}}}{2} \\ &= -\frac{p}{2q} \pm \frac{1}{2}\sqrt{\frac{p^2k - 4qh}{q^2k}} \\ &= -\frac{p}{2q} \pm \frac{1}{2q^2k}\sqrt{q^2k(p^2k - 4qh)} \end{aligned}$$

Note that $q^2k(p^2k - 4qh) \in \mathbb{Z}$, so factor out any perfect square part, calling it n^2, and whatever squarefree integer is left call it d:

$$x = -\frac{p}{2q} \pm \frac{1}{2q^2k}\sqrt{n^2d} = -\frac{p}{2q} \pm \frac{n}{2q^2k}\sqrt{d}$$

Now let $r = -\frac{p}{2q} \in \mathbb{Q}$ and $s = \frac{n}{2q^2k} \in \mathbb{Q}$:

$$x = r \pm s\sqrt{d}$$

And so $K = \mathbb{Q}(\sqrt{d})$

Now assume $\varphi \in G(\mathbb{Q})$
Since φ is a ring homomorphism that fixes $\mathbb{Q}$:

$$\varphi(x) = \phi(r \pm s\sqrt{d}) = \phi(r) \pm \phi(s\sqrt{d}) = r \pm \phi(s)\phi(\sqrt{d}) = r \pm s\phi(\sqrt{d})$$

And so φ is completely determined by what it does to $\sqrt{d}$.

Thus, there are only two $\mathbb{Q}$-automorphisms:

a). id

b). $\sqrt{d} \mapsto -\sqrt{d}$

In other words, the identity and a two-cycle.

Therefore, $\mathrm{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$

Also note that since φ only moves $r + s\sqrt{d}$ where $s \neq 0$:

$$F(G(\mathbb{Q})) = \mathbb{Q}$$

Therefore $Q(\sqrt{d})/\mathbb{Q}$ is Galois.

4). Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is Galois over $\mathbb{Q}$ with Galois group $\mathrm{Gal}(\sqrt{2+\sqrt{2}}/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$.

We can determine the minimum polynomial as follows:

$$\begin{aligned} x &= \sqrt{2+\sqrt{2}} \\ x^2 &= 2+\sqrt{2} \\ x^2 - 2 &= \sqrt{2} \\ x^4 - 4x^2 + 4 &= 2 \\ x^4 - 4x^2 + 2 &= 0 \end{aligned}$$

Let $f(x) = x^4 - 4x^2 + 2$. By Eisenstein ($p = 2$), $f(x)$ is irreducible over $\mathbb{Q}$ and is thus the minimum polynomial for $\mathbb{Q}(\sqrt{2+\sqrt{2}})$. Now, using the quadratic formula twice, we get the four roots for $f(x)$:

$r_1 = \sqrt{2+\sqrt{2}}$
$r_2 = -\sqrt{2+\sqrt{2}}$
$r_3 = \sqrt{2-\sqrt{2}}$
$r_4 = -\sqrt{2-\sqrt{2}}$

Note that:

$$\left(\sqrt{2+\sqrt{2}}\right)^2 = 2+\sqrt{2}$$

and so $\sqrt{2} = -2 + \left(\sqrt{2+\sqrt{2}}\right)^2 \in \mathbb{Q}(\sqrt{2+\sqrt{2}})$.

Furthermore, note that:

$$r_1 r_3 = \left(\sqrt{2+\sqrt{2}}\right)\left(\sqrt{2-\sqrt{2}}\right) = \sqrt{2}$$

Thus:

$$\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} \in \mathbb{Q}(\sqrt{2+\sqrt{2}})$$

This means that all four of the roots are in $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ and thus $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is the splitting field for $f(x)$ over $\mathbb{Q}$.

Therefore K/F is a Galois extension.

$f(x)$ is already depressed with $p = -4$, $q = 0$, and $r = 2$. Thus, the resolvant is:

$$h(x) = x^3 + 8x^2 + 8x = x(x^2 + 8x + 8)$$

with roots 0 and $-4 \pm 2\sqrt{2}$. We are only concerned about the non-rational part so:

$\theta_1 = 0 = (r_1 + r_2)(r_3 + r_3) \in \mathbb{Q}$
$\theta_2 = \sqrt{2} = (r_1 + r_3)(r_2 + r_4) \notin \mathbb{Q}$
$\theta_2 = -\sqrt{2} = (r_1 + r_4)(r_2 + r_3) \notin \mathbb{Q}$

So $\mathrm{Gal}(K/F)$ fixes θ_1 and thus $\mathrm{Gal}(K/F) \leq D_8$. Since the dimension of the extension is 4 it cannot be all of D_8 and so it is either $\mathbb{Z}/4\mathbb{Z}$ or V. But there are 4 distinct roots so we know that $\mathrm{Gal}(K/F)$ has a 4 cycle, as well as a two cycle for conjugation of the roots, so the non-cyclic V is out. Therefore, $\mathrm{Gal}(K/F) \cong \mathbb{Z}/4\mathbb{Z}$.

5). Suppose that K is the splitting field over $\mathbb{Q}$ of a cubic $f(x) \in \mathbb{Q}[x]$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. Prove that all the roots of $f(x)$ are real.

We have the following extension:

$$\begin{tikzcd} K \arrow[d, dash, "3"] \\ \mathbb{Q} \end{tikzcd}$$

Since $\mathbb{Z}/3\mathbb{Z}$ has no proper subgroups, there are no intermediate fields. Now, ABC that $f(x)$ has two complex conjugate roots. This would require a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ of order two to cover conjugation of the complex roots, and thus an intermediate field of dimension 2, which is impossible because $2 \nmid 3$.

Thus, all of the roots of $f(x)$ must be real.

6). Find the Galois group for the splitting field of $x^4 + 2$ over $\mathbb{Q}$.

By Eisenstein ($p = 2$), $x^4 + 2$ is irreducible over $\mathbb{Q}$. It is also already depressed with $p = q = 0$ and $r = 2$. Thus, the corresponding resolvant cubic is:

$$x^3 - 8x = x(x^2 - 8)$$

which has the following roots:

$\theta_1 = 0 = (r_1 + r_2)(r_3 + r_3) \in \mathbb{Q}$
$\theta_2 = \sqrt{8} = (r_1 + r_3)(r_2 + r_4) \notin \mathbb{Q}$
$\theta_2 = -\sqrt{8} = (r_1 + r_4)(r_2 + r_3) \notin \mathbb{Q}$

So $\mathrm{Gal}(K/F)$ fixes θ_1 and thus $\mathrm{Gal}(K/F) \leq D_8$

Consider $(34) \in D_8$:

$(34)\theta_2 = (r_1 + r_4)(r_2 + r_3) = \theta_3$
$(34)\theta_3 = (r_1 + r_3)(r_2 + r_4) = \theta_2$

Thus, $(34) \in \mathrm{Gal}(K/F)$.

Now, consider $(1324) \in \mathrm{Gal}(K/F)$:

$(1324)\theta_2 = (r_3 + r_2)(r_4 + r_1) = \theta_3$
$(1324)\theta_3 = (r_3 + r_1)(r_4 + r_2) = \theta_2$

Thus $(1324) \in \mathrm{Gal}(K/F)$.

Therefore, $\mathrm{Gal}(K/F) = \langle (34), (1324) \rangle = D_8$.

7). Suppose K is an extension of $\mathbb{Q}$ such that $[K : \mathbb{Q}] = 4$ and assume there are no proper non-trivial intermediate fields L with $\mathbb{Q} \subset L \subset K$. Show that K/Q is not Galois.

The lack of proper intermediate fields for a quartic indicates a missing field extension of dimension 2, corresponding to a missing Galois group of order 2 such as conjugation of complex roots. This occurs when the complex roots are not included in the field extension - i.e, the extension is $\mathbb{Q}(\sqrt[4]{d})$ and not the full $\mathbb{Q}(\sqrt[4]{d}, i)$. Thus K is not a splitting field for the minimum polynomial of the extension, and therefore the extension is not Galois.