Solutions for the Galois Theory Problems

Problem 1. Suppose that $\theta \in K$, but $\theta \notin F$. Then $2 = [K : F] = [K : F(\theta)][F(\theta) : F]$ and $[F(\theta) : F] > 1$. It follows that $K = F(\theta)$ and that the minimal polynomial for $\theta$ over $F$ has degree 2. Let $f(x)$ be the minimal polynomial for $\theta$ over $F$. We can write $f(x) = x^2 + ax + b$, where $a, b \in F$.

We know that $f(x) = (x - \theta)(x - \beta)$, where $\theta$ is as above and $\beta \in C$. Thus, we have

$$f(x) = (x - \theta)(x - \beta) = x^2 - (\theta + \beta)x + \theta\beta = x^2 + ax + b$$

and so it follows that $\theta + \beta = -a$ and $\theta\beta = b$.

The splitting field for $f(x)$ over $F$ is $F(\theta, \beta)$. Since $K = F(\theta)$, we have $K \subseteq F(\theta, \beta)$. Now note that $\beta = -a - \theta$ is in the field $K = F(\theta)$. Hence $K$ is a field containing $F$ and also containing $\beta$ as well as $\theta$. Thus, $F(\theta, \beta) \subseteq K$. We have proved that $K = F(\theta, \beta)$.

Thus, $K$ is actually the splitting field over $F$ for $f(x)$, which is a polynomial with coefficients in $F$. Therefore, $K$ is indeed a finite, Galois extension of $F$.

Problem 2.

(a) By the rational root test, the only possible rational roots of $f(x) = x^3 - x - 1$ are $1$ and $-1$. Neither of those numbers is a root. Since $\deg(f(x)) = 3$, it follows that $f(x)$ is irreducible over $\mathbb{Q}$. If $\theta$ is a complex root of $f(x)$, then $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$. It will be useful to make the following observation: Suppose that $F$ is an extension of $\mathbb{Q}$, that $[F : \mathbb{Q}] = 2$, and that $\theta$ is any complex root of $f(x)$. Then $\theta \notin F$. This is clear because $[\mathbb{Q}(\theta) : \mathbb{Q}] = 3$ and hence the degree of $\theta$ over $\mathbb{Q}$ does not divide $[F : \mathbb{Q}]$. Thus, $f(x)$ has no root in $F$ and therefore $f(x)$ is irreducible over $F$. We are again using the fact that $\deg(f(x)) = 3$ to make that conclusion.

In particular, $f(x)$ is irreducible over each of the fields $\mathbb{Q}(\sqrt{-23})$ and $\mathbb{Q}(\sqrt{23})$. Thus, if $F$ is any one of the three fields $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-23})$, or $\mathbb{Q}(\sqrt{23})$, and if $K$ is the splitting field for $f(x)$ over $F$, then we can say that $Gal(K/F)$ is isomorphic to a subgroup of $S_3$ and that $|Gal(K/F)| = [K : F]$ is divisible by 3. This means that $Gal(K/F)$ is isomorphic to either $S_3$ itself, or to $A_3$.

The criterion for deciding between those two possibilities involves the discriminant of $f(x)$. We have

$$d = disc(f(x)) = -4(-1)^3 - 27(-1)^2 = -23.$$
Note that \( d = -23 \) is not a square in \( \mathbb{Q} \). Note also that \(-23\) is not a square in the field \( \mathbb{Q}(\sqrt{23}) \). This follows from the fact that \( \mathbb{Q}(\sqrt{23}) \) is a subfield of \( \mathbb{R} \). It also follows from the lemma proved at the beginning of my solutions for problem set 4.

It follows that \( \text{Gal}(K/F) \) is isomorphic to \( S_3 \) when \( F = \mathbb{Q} \) or \( F = \mathbb{Q}(\sqrt{23}) \).

Obviously, \( d = -23 \) is a square in the field \( F = \mathbb{Q}(\sqrt{-23}) \). Hence, \( \text{Gal}(K/F) \) is isomorphic to \( A_3 \) in this case.

Alternatively, let \( K \) denote the splitting field for \( f(x) \) over \( \mathbb{Q} \). As proved in class, \( K \) must contain \( \sqrt{d} \). Hence, \( K \) must contain \( F = \mathbb{Q}(\sqrt{-23}) \). That is, we have \( \mathbb{Q} \subset F \subset K \).

Hence, as discussed in class, the field \( K \) is also the splitting field for \( f(x) \) over \( F \). Furthermore, the intermediate field \( F \) for the extension \( K/Q \) corresponds to the subgroup \( \text{Gal}(K/F) \) of \( \text{Gal}(K/Q) \) and has index 2. Since \( \text{Gal}(K/Q) \cong S_3 \), it follows that \( \text{Gal}(K/F) \cong A_3 \).

(b) Let \( K \) be the splitting field over \( \mathbb{Q} \) for \( f(x) = x^8 - 1 \). We proved in class that \([K : \mathbb{Q}] = 4\). Also, by problem A in problem set 3, there is an injective group homomorphism \( \rho \) from \( \text{Gal}(K/Q) \) to \( (\mathbb{Z}/8\mathbb{Z})^\times \). Both groups have order 4 and so \( \rho \) is an isomorphism. Thus, \( \text{Gal}(K/Q) \) is isomorphic to \( (\mathbb{Z}/8\mathbb{Z})^\times \), which is an abelian group in which every element has order 1 or 2. Thus, \( \text{Gal}(K/Q) \) is isomorphic to \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) as a group.

We also know that \( i \in K \) and hence that \( \mathbb{Q}(i) \subset K \). We have \( \mathbb{Q} \subset \mathbb{Q}(i) \subset K \).

Also, \( 4 = [K : \mathbb{Q}] = [K : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2[K : \mathbb{Q}(i)] \). These remarks show that \( K \) is also the splitting field for \( f(x) \) over \( \mathbb{Q}(i) \) and that \([K : \mathbb{Q}(i)] = 2\). It follows that \( \text{Gal}(K/\mathbb{Q}(i)) \) has order 2. Hence that Galois group is isomorphic to \( \mathbb{Z}/2\mathbb{Z} \).

(c) Let \( f(x) = x^3 - x^2 - 4 \). Note that \( f(2) = 0 \). Thus, \( f(x) \) is reducible over \( \mathbb{Q} \). In fact, we have

\[
f(x) = (x - 2)(x^2 + x + 2).
\]

It follows that the splitting fields over \( \mathbb{Q} \) for \( f(x) \) and for \( g(x) = x^2 + x + 2 \) coincide. The rational root test shows that \( g(x) \) is irreducible over \( \mathbb{Q} \).

Let \( K \) denote the splitting field over \( \mathbb{Q} \) for \( f(x) \). If \( \theta \) is a complex root of \( g(x) \), then \( K = \mathbb{Q}(\theta) \), as explained in the solution for problem 1. Thus, \([K : \mathbb{Q}] = 2 \) and \( \text{Gal}(K/\mathbb{Q}) \) is of order 2. The Galois group is isomorphic to \( \mathbb{Z}/2\mathbb{Z} \).
As an incidental remark, we have $K = \mathbb{Q}(\sqrt{-7})$.

(d) Let $f(x) = x^3 - x^2 - 2x + 1$. The rational root test shows that the only possible roots of $f(x)$ in $\mathbb{Q}$ are 1 or $-1$. Neither is actually a root. Since $\deg(f(x)) = 3$, it follows that $f(x)$ is irreducible over $\mathbb{Q}$. Thus, if $K$ denotes the splitting field over $\mathbb{Q}$ for $f(x)$, then $Gal(K/\mathbb{Q})$ is isomorphic either to $S_3$ or to $A_3$.

Using a formula from the handout about discriminants, and taking $a_1 = -1$, $a_2 = -2$, and $a_3 = 1$, we have

$$disc(f(x)) = 49.$$

Note that 49 is a square in $\mathbb{Q}$. It follows that $Gal(K/\mathbb{Q})$ is isomorphic to $A_3$, a cyclic group of order 3.

**Problem 3.** All of the complex roots of the polynomial $x^{17} - 1$ are powers of $\omega$, which is one of the complex roots of that polynomial. It follows that $K = \mathbb{Q}(\omega)$ is the splitting field over $\mathbb{Q}$ for $x^{17} - 1$. Therefore, $K$ is a Galois extension of $\mathbb{Q}$. Furthermore, according to problem F in problem set 4, we know that there is an isomorphism

$$\rho : Gal(K/\mathbb{Q}) \rightarrow (\mathbb{Z}/17\mathbb{Z})^\times.$$ 

Now $(\mathbb{Z}/17\mathbb{Z})^\times$ has order 16. In fact, it is a cyclic group of order 16. One sees this just by verifying that $3 + 17\mathbb{Z}$ generates the group $(\mathbb{Z}/17\mathbb{Z})^\times$. For that verification, it suffices to note that $3^8 = 6561$ and $6561 \equiv -1 \pmod{17}$. This means that $3 + 17\mathbb{Z}$ is an element of $(\mathbb{Z}/17\mathbb{Z})^\times$ whose order does not divide 8. That element must therefore have order 16.

Since $\rho$ is an isomorphism, we can now say that $G = Gal(K/\mathbb{Q})$ is a cyclic group of order 16. This fact implies that $G$ has a unique subgroup $H$ of order 2. By the Fundamental Theorem of Galois Theory, it follows that there is a unique intermediate field $L$ for the extension $K/\mathbb{Q}$ such that $Gal(K/L)$ has order 2. We have $H = Gal(K/L)$. Furthermore, $[K : L] = 2$ and so $[L : \mathbb{Q}] = 8$. Since $H = Gal(K/L)$ is a normal subgroup of $G$, it follows that $L$ is a Galois extension of $\mathbb{Q}$.

We can also say that $Gal(L/\mathbb{Q}) \cong G/H$. Now $G$ is a cyclic group, and so $G/H$ must also be a cyclic group. Its order is $[G : H] = 8$.

To find a generator for $L$ over $\mathbb{Q}$, consider the minimal polynomial $m(x)$ for $\omega$ over $L$. The only element in $(\mathbb{Z}/17\mathbb{Z})^\times$ of order 2 is $-1 + 17\mathbb{Z}$. Let $\tau$ denote the corresponding element of $Gal(K/\mathbb{Q})$. Then $H = \langle \tau \rangle$, the cyclic subgroup of $G$ generated by $\tau$. Using the definition of the isomorphism $\rho$, we have

$$\tau(\omega) = \omega^{-1}.$$
As explained in class, it follows that the minimal polynomial for $\omega$ over $L$ is given by
\[ m(x) = (x-\omega)(x-\tau(\omega)) = (x-\omega)(x-\omega^{-1}) = x^2 - (\omega + \omega^{-1})x + \omega\omega^{-1} = x^2 - \beta x + 1, \]
where $\beta = \omega + \omega^{-1}$. In particular, note that $\beta$ must be an element of the field $L$.

Let $F = \mathbb{Q}(\beta)$. Then we have $\mathbb{Q} \subseteq F \subseteq L \subseteq K$. By the degree formula, we have
\[ [K : F] = [K : L][L : F]. \]

Now $[K : L] = 2$. But notice that $K = F(\omega)$, that $\omega$ is a root of the quadratic polynomial $m(x)$, and that $m(x)$ has coefficients in the field $F$. It follows that $[K : F] \leq 2$. Thus, we see that $[L : F] = 1$ and we must have $L = F$. That is, we have $L = \mathbb{Q}(\beta)$.

We add one incidental remark. Notice that $\beta = 2\cos(\frac{2\pi}{17})$. Thus, the field $L$ described above is generated over $\mathbb{Q}$ by $\cos(\frac{2\pi}{17})$.

**Problem 4.** By definition, $M = \mathbb{Q}(\kappa, \lambda)$ is the field $KL$, the compositum of the fields $K$ and $L$. Since $K$ and $L$ are finite Galois extensions of $\mathbb{Q}$, there exists polynomials $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$ such that $K$ is the splitting field over $\mathbb{Q}$ for $f(x)$ and $L$ is the splitting field over $\mathbb{Q}$ for $g(x)$. Thus, by definition, $K$ is the smallest extension of $\mathbb{Q}$ containing all the roots of $f(x)$ and $L$ is the smallest extension of $\mathbb{Q}$ containing all the roots of $g(x)$.

It follows that $M = KL$ is the smallest extension of $\mathbb{Q}$ containing all the roots of $f(x)g(x)$. Furthermore, $f(x)g(x) \in \mathbb{Q}[x]$. Thus, we can say that $M$ is the splitting field over $\mathbb{Q}$ for $f(x)g(x)$. Therefore, $M$ is indeed a finite, Galois extension of $\mathbb{Q}$.

Note that $M = KL$ contains both $K$ and $L$. Hence $K$ and $L$ are intermediate fields for the extension $M/\mathbb{Q}$. Both $K$ and $L$ are Galois extensions of $\mathbb{Q}$. Thus, we can use the restriction maps to define homomorphisms from $\text{Gal}(M/\mathbb{Q})$ to $\text{Gal}(K/\mathbb{Q})$ and to $\text{Gal}(L/\mathbb{Q})$. We can define one single homomorphism
\[ \phi : \text{Gal}(M/\mathbb{Q}) \longrightarrow \text{Gal}(K/\mathbb{Q}) \times \text{Gal}(L/\mathbb{Q}) \]
by
\[ \phi(\sigma) = (\sigma|_K, \sigma|_L), \]
for all $\sigma \in \text{Gal}(M/\mathbb{Q})$.

We omit the straightforward verification that $\phi$ is a group homomorphism. Furthermore, since $M = \mathbb{Q}(\kappa, \lambda)$, it follows that an element $\sigma \in \text{Gal}(M/\mathbb{Q})$ is completely determined if one knows $\sigma(\kappa)$ and $\sigma(\lambda)$. Consequently, such a $\sigma$ is completely determined if one knows $\sigma|_K$ and $\sigma|_L$. Consequently, the homomorphism $\phi$ is injective.
The above arguments are rather general. Suppose now that \([K : \mathbb{Q}] = 3\) and \([L : \mathbb{Q}] = 3\).

By assumption, \(K\) and \(L\) are Galois extensions of \(\mathbb{Q}\). Both \(\text{Gal}(K/\mathbb{Q})\) and \(\text{Gal}(L/\mathbb{Q})\) are cyclic groups of order 3. They are isomorphic to \(\mathbb{Z}/3\mathbb{Z}\).

The injective homomorphism \(\phi\) defined above shows that \(\text{Gal}(M/\mathbb{Q})\) is isomorphic to a subgroup of \(\text{Gal}(K/\mathbb{Q}) \times \text{Gal}(L/\mathbb{Q})\), which is a group of order 9. Therefore, \(|\text{Gal}(M/\mathbb{Q})|\) divides 9. It follows that \([M : \mathbb{Q}]\) divides 9. Since \(\mathbb{Q} \subset K \subset M\), we also can say that \([M : \mathbb{Q}]\) is divisible by \([K : \mathbb{Q}] = 3\). Therefore, either \([M : \mathbb{Q}] = 3\) or \([M : \mathbb{Q}] = 9\).

We will show that \([M : \mathbb{Q}] = 9\). Assume to the contrary that \([M : \mathbb{Q}] = 3\). Since \(K\) and \(L\) are extensions of \(\mathbb{Q}\) of degree 3 and both are subfields of \(M\), it would follow that \(K = M\) and \(L = M\). Hence, it would follow that \(K = L\). However, it is assumed in this problem that \(K \neq L\). Thus, we have a contradiction. This means that \([M : \mathbb{Q}] = 9\).

The homomorphism \(\phi\) is injective. Both \(\text{Gal}(M/\mathbb{Q})\) and \(\text{Gal}(K/\mathbb{Q}) \times \text{Gal}(L/\mathbb{Q})\) have order 9. It follows that \(\phi\) is an isomorphism. Therefore, \(\text{Gal}(M/\mathbb{Q})\) is indeed isomorphic to \(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\), as stated.

**Problem 5.** This problem is closely related to problem 3. Instead of considering the splitting field for \(x^{17} - 1\), we consider the splitting field for \(x^{29} - 1\). Denote the splitting field over \(\mathbb{Q}\) for \(x^{29} - 1\) by \(M\). This time, we have a group isomorphism \(\rho : \text{Gal}(M/\mathbb{Q}) \rightarrow (\mathbb{Z}/29\mathbb{Z})^\times\).

The group \((\mathbb{Z}/29\mathbb{Z})^\times\) is a cyclic group of order 28. It is generated by \(2 + 29\mathbb{Z}\). To verify this, it suffices to show that \(2^{14} \not\equiv 1 \pmod{29}\) and \(2^4 \not\equiv 1 \pmod{29}\), which we leave to the reader. Let \(G = \text{Gal}(M/\mathbb{Q})\). Then \(G\) is a cyclic group of order 28.

If \(H\) is the unique subgroup of \(G\) of order 2, then \(G/H\) is a cyclic group of order 14 and hence is isomorphic to \(\mathbb{Z}/14\mathbb{Z}\). Thus, if \(K = MH\), then we have \(\text{Gal}(K/\mathbb{Q}) \cong G/H\). Hence, \(\text{Gal}(K/\mathbb{Q})\) is isomorphic to \(\mathbb{Z}/14\mathbb{Z}\).

**Problem 6.** The complex roots of \(f(x)\) are

\[
-\frac{1}{2} + \frac{\sqrt{-3}}{2}, \quad -\frac{1}{2} - \frac{\sqrt{-3}}{2}, \quad -\frac{1}{2} + \frac{\sqrt{5}}{2}, \quad -\frac{1}{2} - \frac{\sqrt{5}}{2}.
\]

The field \(F\) is generated over \(\mathbb{Q}\) by the above four numbers. Now one sees easily that we have \(F = \mathbb{Q}(\sqrt{-3}, \sqrt{5})\). The field \(F\) is a Galois extension of \(\mathbb{Q}\) and, just as for the field \(\mathbb{Q}(\sqrt{2}, \sqrt{3})\) discussed in class, one finds that \([F : \mathbb{Q}] = 4\).

The polynomial \(g(x)\) has degree 3 and is irreducible over \(\mathbb{Q}\). This follows from the rational root test. Therefore, \(\beta\) has degree 3 over \(\mathbb{Q}\). Hence, for \(K = \mathbb{Q}(\beta)\), we have \([K : \mathbb{Q}] = 3\).
Now $F \cap K$ is a subfield of $F$ and also a subfield of $K$. Of course, the field $F \cap K$ contains $\mathbb{Q}$. It follows that $[F \cap K : \mathbb{Q}]$ divides both $[F : \mathbb{Q}] = 4$ and $[K : \mathbb{Q}] = 3$. Therefore, $[F \cap K : \mathbb{Q}] = 1$. Hence, we have $F \cap K = \mathbb{Q}$.

Now we will consider $F \cap L$. Here $L$ is the splitting field over $\mathbb{Q}$ for $g(x)$. Since $g(x)$ has degree 3 and is irreducible over $\mathbb{Q}$, we know that $Gal(L/\mathbb{Q})$ is isomorphic either to $S_3$ or to $A_3$. The discriminant of $g(x)$ is

$$d = -4 \cdot 3^3 - 27 \cdot 1^2 = -5 \cdot 27 = -135.$$ 

Thus, $L$ contains the field $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{-15})$, we have $Gal(L/\mathbb{Q}) \cong S_3$, and $[L : \mathbb{Q}] = 6$.

Notice that $\sqrt{-15} = \sqrt{5}\sqrt{-3}$ is in the field $F$. Hence we have $\mathbb{Q}(\sqrt{-15}) \subset F$. Also, as we found above, we have $\mathbb{Q}(\sqrt{-15}) \subset L$. Thus, we have

$$\mathbb{Q}(\sqrt{-15}) \subseteq F \cap L.$$ 

We will prove equality by verifying that both of these fields have degree 2 over $\mathbb{Q}$. This is clear for $\mathbb{Q}(\sqrt{-15})$. The above inclusion shows that $[F \cap L : \mathbb{Q}]$ is divisible by 2.

Now $F \cap L$ is a subfield of both $F$ and $L$, which are extensions of $\mathbb{Q}$ of degree 4 and 6, respectively. It follows that $[F \cap L : \mathbb{Q}]$ divides both 4 and 6. Hence $[F \cap L : \mathbb{Q}] \leq 2$. Since $[F \cap L : \mathbb{Q}]$ is divisible by 2, it follows that we indeed have $[F \cap L : \mathbb{Q}] = 2$. Consequently, we have proved that $F \cap L = \mathbb{Q}(\sqrt{-15})$.

**Problem 7.** We are given that $K$ is a finite, Galois extension of $\mathbb{Q}$. Let $G = Gal(K/\mathbb{Q})$. By assumption, we have $G \cong S_4$. Now $S_4$ contains a subgroup of order 6, namely

$$\{ g \in S_4 \mid g(4) = 4 \},$$ 

a subgroup of $S_4$ which is isomorphic to $S_3$. It follows that $G$ has a subgroup $H$ such that $H \cong S_3$. We let $L$ denote $K^H$. Note that

$$[L : \mathbb{Q}] = [G : H] = \frac{|G|}{|H|} = \frac{24}{6} = 4.$$ 

By the Primitive Element Theorem, we have $L = \mathbb{Q}(\beta)$ for some $\beta \in \mathbb{C}$. Since $[L : \mathbb{Q}] = 4$, it follows that $\beta$ has degree 4 over $\mathbb{Q}$. Let $g(x)$ be the minimal polynomial for $\beta$ over $\mathbb{Q}$.

We have $g(x) \in \mathbb{Q}[x]$ and $\deg(g(x)) = 4$. Let $M$ denote the splitting field for $g(x)$ over $\mathbb{Q}$. Since $K$ is a Galois extension of $\mathbb{Q}$ and $\beta \in K$, it follows that all of the complex roots of $g(x)$ are also in $K$. We proved this in class. Thus, it follows that $M \subseteq K$. Also, $L \subseteq M$. Thus, we have $L \subseteq M \subseteq K$. 
By the degree formula, we have $[K : L] = [K : M][M : L]$. Also, $Gal(K/L) = H \cong S_3$. Therefore, $[K : L] = 6$. Thus, $[K : M]$ divides 6.

Since $M$ is a Galois extension of $\mathbb{Q}$, it follows that $Gal(K/M)$ is a normal subgroup of $G = Gal(K/\mathbb{Q})$. But $|Gal(K/M)| = [K : M]$ divides 6. Recall that $S_4$ has normal subgroups only of orders 24, 12, 4, and 1. Now, 24, 12, and 4 don’t divide 6. Therefore, we can conclude that $|Gal(K/M)| = 1$. Hence $Gal(K/M) = \{id_G\}$. This means that $M = K$. That is, the splitting field over $\mathbb{Q}$ for $g(x)$ is indeed the field $K$.

**Problem 8.** It was unfortunately not specified in the problem, but we want $f(x)$ to be a polynomial of degree 3.

Let $G = Gal(K/\mathbb{Q})$. We are given that $G \cong S_4$. Now $S_4$ has a subgroup of order 8, namely the dihedral group $D_8$. Thus, $G$ also has a subgroup of order 8. Let $H$ be such a subgroup.

Now let $L = K^H$. We have $H = Gal(K/L)$. Thus, $[K : L] = |H| = 8$. Furthermore, we have $[L : \mathbb{Q}] = [G : H] = 3$.

Suppose that $\theta \in L$, but $\theta \not\in \mathbb{Q}$. Since $[L : \mathbb{Q}] = 3$, it follows that $L = \mathbb{Q}(\theta)$. Let $f(x)$ be the minimal polynomial for $\theta$ over $\mathbb{Q}$. Then $f(x) \in \mathbb{Q}[x]$, $f(x)$ has degree 3, and $f(x)$ is irreducible over $\mathbb{Q}$.

One root of $f(x)$ is $\theta$. Now $\theta \in L$ and $L \subset K$. Hence $\theta \in K$. Since $K$ is a Galois extension of $\mathbb{Q}$, it follows that all of the roots of $f(x)$ must be in $K$. The polynomial $f(x)$ has all of the requested properties in this problem.