(1) Let $G$ be a finite abelian group. Prove that there exists an abelian extension of $\mathbb{Q}$ with the Galois group $G$.

Proof. If $G$ is a finite abelian group then we know that we can write

$$G \cong \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_k.$$ 

By Dirichlet’s theorem in number theory we know that for any fixed positive integer $n$, there exists an infinite amount of prime numbers of the form $kn + 1$ where $k$ is a positive integer. This shows that for each $n_i$, we can choose distinct primes $p_i$ such that $p_i = k_i n_i + 1$. In other words, $n_i | p_i - 1$. Since $(\mathbb{Z}/p_i)^\ast$ is a cyclic group of order $p_i - 1$ we can find a subgroup $H_i$ of order $(\mathbb{Z}/p_i)^\ast/H_i$ is a cyclic group of order $n_i$ and is therefore isomorphic to $\mathbb{Z}/n_i$. This shows that we can write

$$G \cong (\mathbb{Z}/p_1)^\ast/H_1 \times (\mathbb{Z}/p_2)^\ast/H_2 \times \cdots \times (\mathbb{Z}/p_k)^\ast/H_k$$

Let $n = p_1 \cdots p_k$, then since the $p_i$ are distinct we know that $(\mathbb{Z}/p_1)^\ast \times \cdots \times (\mathbb{Z}/p_k)^\ast \cong (\mathbb{Z}/n)^\ast$. Let $H$ be the subgroup of $(\mathbb{Z}/n)^\ast$ that corresponds to $H_1 \times \cdots \times H_k$, then we see that

$$G \cong (\mathbb{Z}/n)^\ast/H.$$ 

Let $\xi$ be a primitive $n$-th root of unity. Then we know that $\text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) = (\mathbb{Z}/n)^\ast$. Let $E = \mathbb{Q}(\xi)^H$ be the fixed field of $H$. Then $E$ is an extension of $\mathbb{Q}$ and since $(\mathbb{Z}/n)^\ast$ is abelian, we know that $H$ is a normal subgroup which implies that $E/\mathbb{Q}$ is Galois. Moreover, we know that

$$\text{Gal}(E/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})/H \cong (\mathbb{Z}/n)^\ast/H \cong G.$$ 

This shows that any finite abelian group is the Galois group of some extension of $\mathbb{Q}$. \qed

(2) Let $K/\mathbb{Q}$ be a finite extension of $\mathbb{Q}$. Let $G$ be a non-trivial finite abelian group. Prove that there exist infinitely many abelian extensions of $K$ with Galois group $G$.

Proof. Just as in part (a) above, write $G = \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_k$. Then by Dirichlet’s theorem we know that we can find an infinite number of primes $p_i$ such that $n_i | p_i - 1$ and we can therefore construct an infinite number of $k$-tuples $\{(p_1, p_2, \ldots, p_k)\}$ such that $(p_1, p_2, \ldots, p_k) \cap (p'_1, p'_2, \ldots, p'_k) = \emptyset$. Then we saw that we can construct a Galois extension $E$ with group $G$ such that

$$\mathbb{Q} \subset E \subset \mathbb{Q}(\xi_{p_1 \cdots p_k}),$$

where $\xi_{p_1 \cdots p_k}$ is a $p_1 \cdots p_k$-th primitive root of unity. Since this can be done for any of the $k$-tuple of primes chosen above, we potentially have an infinite number of distinct
extensions of \( \mathbb{Q} \) with Galois group \( G \). Let \((p_1, \ldots, p_k)\) and \((p'_1, \ldots, p'_k)\) be two distinct \( k \)-tuple of primes and let \( E \) and \( E' \) be the subextensions of \( \mathbb{Q}(\xi_{p_1} \cdots p_k) \) and \( \mathbb{Q}(\xi_{p'_1} \cdots p'_k) \) respectively. Since \( \mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m) = \mathbb{Q} \) for \((n, m) = 1\) we see that since all of the \( p_i \) are different than the \( p_j \) that

\[
\mathbb{Q} \subset E \cap E' \subset \mathbb{Q}(\xi_{p_1} \cdots p_k) \cap \mathbb{Q}(\xi_{p'_1} \cdots p'_k) = \mathbb{Q}
\]

which shows that \( E \) and \( E' \) are distinct extensions of \( \mathbb{Q} \) with Galois groups \( G \). Let \( \{E_\alpha\} \) be the set of extensions of \( \mathbb{Q} \) with Galois group \( G \) constructed above using the \( k \)-tuples of primes. \( \mathbb{K}/\mathbb{Q} \) is a finite extension and since we are in characteristic 0 we know that it is separable. Therefore, there are only a finite number of fields \( L \) such that \( \mathbb{Q} \subset L \subset \mathbb{K} \). Consider the following diagram,

\[
\begin{array}{c}
\mathbb{K} \\
\downarrow \downarrow \\
\mathbb{K} \cap E_\alpha \\
\downarrow \\
\mathbb{Q}
\end{array}
\]

Since \( E_\alpha/\mathbb{Q} \) is Galois we know that \( KE_\alpha/\mathbb{K} \) is Galois and moreover,

\[
\text{Gal}(KE_\alpha/\mathbb{K}) = \text{Gal}(E_\alpha/\mathbb{K} \cap E_\alpha).
\]

\( \mathbb{K} \cap E_\alpha \) is a subfield of \( \mathbb{K} \) for each \( E_\alpha \) and we know that there are only finitely many subfields of \( \mathbb{K}/\mathbb{Q} \). Also, since \( (\mathbb{K} \cap E_\alpha) \cap (\mathbb{K} \cap E_\beta) = \mathbb{K} \cap (E_\alpha \cap E_\beta) = \mathbb{K} \cap \mathbb{Q} = \mathbb{Q} \) we see that only a finite number of the \( E_\alpha \) can have intersection with \( \mathbb{K} \) to be more than \( \mathbb{Q} \). Therefore, there is an infinite number of the \( E_\alpha \) such that \( \mathbb{K} \cap E_\alpha = \mathbb{Q} \). For these \( E_\alpha \) we see then that

\[
\text{Gal}(KE_\alpha/\mathbb{K}) = \text{Gal}(E_\alpha/\mathbb{K} \cap E_\alpha) = \text{Gal}(E_\alpha/\mathbb{Q}) = G
\]

which shows that there are an infinite number of distinct Galois extensions of \( \mathbb{K} \) that have Galois group \( G \).

**Addition** (Julia). We need to take care of the following detail pointed out by Jim: prove that there are infinitely many \( \alpha_i \) such that \( KE_{\alpha_i}, KE_{\alpha_j} \) are different extensions of \( \mathbb{K} \).

**Lemma 0.1.** Let \( m, n, \ell \) be mutually relatively prime. Then \( \mathbb{Q}(\xi_{mn}) \cap \mathbb{Q}(\xi_{m\ell}) = \mathbb{Q}(\xi_m) \).

**Proof.** Exercise \( \square \)

**Lemma 0.2.** Let \( \mathbb{K}/\mathbb{Q} \) be a finite extension, and let \( \{m_1, \ldots, m_i, \ldots\} \) be an infinite sequence of positive integers such that

(a) \( (m_i, m_j) = 1 \) for any pair of distinct indices \( (i, j) \).
(b) \( K \cap Q(\xi_{m_i}) = Q \) for any \( m_i \).

Then there exist only finitely many pairs \( i, j \) such that \( K \cap Q(\xi_{m_im_j}) \neq Q \).

**Proof.** Let \( L_s \) be a non-trivial subextension of \( K, \; Q \subset L_s \subset K \). Suppose \( L_s \subset Q(\xi_{m_im_j}) \) and \( L_s \subset Q(\xi_{m_km_l}) \). Then

\[
L_s \subset Q(\xi_{m_im_j}) \cap Q(\xi_{m_km_l})
\]

If all four numbers \( m_i, m_j, m_k, m_l \) are different, then \( (m_i, m_j, m_k, m_l) = 1 \), and, hence, \( Q(\xi_{m_im_j}) \cap Q(\xi_{m_km_l}) = Q \), a contradiction. Without loss of generality, we may assume that \( m_i = m_k \). Then

\[
L_s \subset Q(\xi_{m_im_j}) \cap Q(\xi_{m_im_l}) = Q(\xi_{m_i})
\]

where the last equality holds by Lemma 0.1. This implies that \( K \cap Q(\xi_{m_i}) \) contains \( L_s \) and, hence, is nontrivial. This contradicts our hypothesis (b). Hence, for any \( L_s \) there is at most one pair \( (i, j) \) such that \( L_s \subset Q(\xi_{m_im_j}) \). Since \( K/Q \) is separable, there are only finitely many different subfields \( L_s \), which finishes the proof of the lemma. \( \square \)

Lemma 0.2 implies that by removing finitely many \( k \)-tuples \( (p_1, \ldots, p_k) \) we can ensure that \( K \cap Q(\xi_{m_i}) \) contains \( L_s \) and, hence, is nontrivial. This contradicts our hypothesis (b). Hence, for any \( L_s \) there is at most one pair \( (i, j) \) such that \( L_s \subset Q(\xi_{m_im_j}) \). Since \( K/Q \) is separable, there are only finitely many different subfields \( L_s \), which finishes the proof of the lemma. \( \square \)

Consider the diagram

\[
\begin{array}{ccc}
K(\xi_{m_n}) & \rightarrow & Q(\xi_{m_n}) \\
\downarrow & & \downarrow \\
K & \rightarrow & Q(\xi_{m_n}) \\
\downarrow & & \downarrow \\
Q & & \\
K(\xi_{m}) & \leftarrow & Q(\xi_{m}) \\
\downarrow & & \downarrow \\
K & \leftarrow & Q \\
\end{array}
\]

Since \( K \cap Q(\xi_{m_n}) = Q \), and \( Q(\xi_{m_n})/Q \) is Galois, we get

\[
[K(\xi_{m_n}) : K] = [Q(\xi_{m_n}) : Q] = \phi(mn)
\]

Now consider a tower of extensions

\[
\begin{array}{ccc}
K(\xi_{m_n}) & \rightarrow & K(\xi_{m}) \\
\downarrow & & \downarrow \\
K & \rightarrow & K \\
\end{array}
\]

The degree of the bottom extension is \( \phi(m) \) (it follows as above from the fact that \( K \cap Q(\xi_{m}) = Q \)). The degree of \( K(\xi_{m_n})/K(K(\xi_{m})) = \phi(mn) \). Hence,

\[
[K(\xi_{m_n}) : K(\xi_{m})] = \phi(m)
\]
and similarly
\[ [K(\xi_m \xi_n) : K(\xi_n)] = \phi(n) \]

Now consider another diagram

\[ \begin{array}{ccc}
K(\xi_m \xi_n) & \phi(n) & K(\xi_n) \\
& \phi(m) & \\
K(\xi_m) & & K(\xi_n) \\
& \phi(m) & \\
& & K \\
\phi(n) & & \phi(n)
\end{array} \]

Since \( K(\xi_n)/K \) is Galois, we have
\[ [K(\xi_m \xi_n) : K(\xi_m)] = [K(\xi_n) : K(\xi_m) \cap K(\xi_n)]. \]

It follows that
\[ [K(\xi_n) : K(\xi_m) \cap K(\xi_n)] = \phi(n) = [K(\xi_n) : K]. \]
Hence, \( K(\xi_m) \cap K(\xi_n) = K. \)