1. Let $\epsilon = e^{2\pi i/18}$. Now assume (and this is true) that $[Q(\epsilon) : Q] = 6$. Let $p(x) \in Q[x]$ be the minimal polynomial for $\epsilon$.

(a) What is the degree of $p(x)$?

Solution: We always have that the degree of $K(\alpha)$ is the same as the degree of the minimal polynomial for $\alpha$ in $K[x]$. Thus it is of degree 6.

(b) Give all the roots of $p(x)$.

Solution: From the midterm only $\epsilon, \epsilon^5, \epsilon^7, \epsilon^{11}, \epsilon^{13}, \epsilon^{17}$ can be roots but as $p(x)$ has degree 6 it has six roots (recall that we showed that an irreducible polynomial (provided the characteristic was 0) must have distinct roots) and so these are the roots, all the roots, nothing but the roots.

(c) Describe all $\sigma \in \Gamma[Q(\epsilon) : Q]$ in a nice way. Give a table of all products in $\Gamma[Q(\epsilon) : Q]$.

Solution: Set $S = \{1, 5, 7, 11, 13, 17\}$. For each $j \in S$ we have $\sigma_j \in \Gamma[Q(\epsilon) : Q]$ determined by $\sigma_j(\epsilon) = \epsilon^j$. Then $\sigma_j \sigma_k(\epsilon) = \sigma_k(\epsilon^j) = \epsilon^{jk}$ so $\sigma_j \sigma_k = \sigma_{jk}$ where the index is determined modulo 18. The table is (writing $j$ for $\sigma_j$):

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>7</td>
<td>11</td>
<td>13</td>
<td>17</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>7</td>
<td>17</td>
<td>1</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>17</td>
<td>13</td>
<td>5</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>1</td>
<td>5</td>
<td>13</td>
<td>17</td>
<td>7</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>11</td>
<td>1</td>
<td>17</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>17</td>
<td>17</td>
<td>13</td>
<td>11</td>
<td>7</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

(d) What well known group is $\Gamma[Q(\epsilon) : Q]$ isomorphic to? Give the isomorphism explicitly.

Solution: This is a cyclic group on six elements. We can take 5 as a generator. Then $\Gamma[Q(\epsilon) : Q]$ is isomorphic to $(Z_6, +)$ with $\phi : (Z_6, +) \to \Gamma[Q(\epsilon) : Q]$ an isomorphism with $\phi(0) = e$, $\phi(1) = \sigma_5$, $\phi(2) = \sigma_5^2 = \sigma_7$, $\phi(3) = \sigma_5^3 = \sigma_{17}$, $\phi(4) = \sigma_5^4 = \sigma_{13}$, $\phi(5) = \sigma_5^5 = \sigma_{11}$. One way to see this is to note that $\Gamma[Q(\epsilon) : Q]$ is Abelian and to know that $(Z_6, +)$ is the only Abelian group on 6 elements.

2. Let $K = Q(\sqrt{a_1}, \ldots, \sqrt{a_s})$ with $a_1, \ldots, a_s \in Q$. 

Honors Algebra II
Assignment 8 Solutions
(a) Give an upper bound on \([K : Q]\).
Solution: \(2^s\) from the Tower Theorem. But it might be less, for example \(Q(\sqrt{2}, \sqrt{3}, \sqrt{6})\).

(b) Let \(\sigma \in \Gamma[K : Q]\). Prove \(\sigma^2 = e\).
Solution: For each \(1 \leq i \leq s\), \(\sigma(\sqrt{a_s}) = \epsilon_s \sqrt{a_s}\) with \(\epsilon_s \in \{-1, +1\}\). Then

\[
\sigma^2(\sqrt{a_s}) = \sigma(\epsilon_s \sqrt{a_s}) = \epsilon_s^2 \sqrt{a_s} = \sqrt{a_s}
\]

As \(\sigma^2\) preserves a set of elements that generate \(K\) it preserves all of \(K\) so it is the identity.

(c) Let \(\sigma, \tau \in \Gamma[K : Q]\). Prove \(\sigma \tau = \tau \sigma\).
Solution: With \(\sigma(\sqrt{a_s}) = \epsilon_s \sqrt{a_s}\) and \(\tau(\sqrt{a_s}) = \gamma_s \sqrt{a_s}\) we have \(\sigma(\tau(\sqrt{a_s})) = \sigma(\gamma_s \sqrt{a_s}) = \epsilon_s \gamma_s \sqrt{a_s}\) and \(\tau(\sigma(\sqrt{a_s})) = \tau(\epsilon_s \sqrt{a_s}) = \gamma_s \epsilon_s \sqrt{a_s}\) so \(\sigma \tau\) and \(\tau \sigma\) agree on all \(\sqrt{a_s}\) and so they are equal.

3. Let \(p(x) \in Q[x]\) be an irreducible cubic with roots \(\alpha, \beta, \gamma \in C\). Let \(K = Q(\alpha, \beta, \gamma)\). Suppose \(\sqrt{a} \in K\) where \(a \in Q\) and \(\sqrt{a} \notin Q\). Set \(L = Q(\sqrt{a})\).

(a) Prove \(p(x)\) is still irreducible when considered in \(L[x]\). (Hint: When cubics reduce they have a root.)
Solution: If \(p(x)\) reduced it would have a root, say \(\alpha\). That is \(\alpha \in L\). But we already have \([Q(\alpha) : Q] = 3\) and all \(\beta \in L\) have \(Q(\beta) : Q \leq 2\), a contradiction.

(b) Prove \([K : Q] = 6\).
Solution: We showed in general that when \(p(x) \in Q[x]\) has roots \(\alpha_1, \ldots, \alpha_n\) then \([Q(\alpha_1, \ldots, \alpha_n) : Q] \leq n!\), in this case \(3! = 6\). For the lower bound \(L \subset K\) with \([L : Q] = 2\). In \(L[x]\), \(p(x)\) is irreducible so \([L(\alpha) : L] = 3\) and hence \([L(\alpha) : Q] = 6\) and\([K : Q] \geq [L(\alpha) : Q] = 6\). Indeed, this shows that \(K = L(\alpha)\), so that \(\beta\) can be expressed in terms of \(\alpha\) and \(\sqrt{a}\).

4. Set \(\alpha = 2^{1/4}\), \(\beta = i\alpha\), \(\gamma = -\alpha\), \(\delta = -i\alpha\). Set \(p(x) = x^4 - 2\). Set \(K = Q(\alpha, \beta, \gamma, \delta)\). Set \(L = Q(i)\). Set \(\Gamma = \Gamma[K : Q]\), the Galois Group of \(K\) over \(Q\).

(a) Show that \(p(x)\) is irreducible in \(Q[x]\).
Solution: Eisenstein’s Criterion! Two divides coefficients 0,0,0,-2 and four doesn’t divide -2 and 2 doesn’t divide the lead coefficient one.
(b) Give the factorization of \( p(x) \) into irreducible factors in \( K[x] \).

**Solution:** As \( \alpha, \beta, \gamma, \delta \) are roots and all are in \( K \),

\[ p(x) = (x - \alpha)(x - \beta)(x - \gamma)(x - \delta) \]

(c) Show that \( p(x) \) is irreducible in \( L[x] \). (As \( p(x) \) is quartic it is not enough to look for factors as, a priori, it could be the product of two quadratics. But given your factorization for problem 4b any factorization over the smaller field \( L \) must come from joining together factors from 4b. Show that none of them work.)

**Solution:** As none of \( \alpha, \beta, \gamma, \delta \) is in \( L \) if \( p(x) \) reduced it would into two quadratics and one would be either \( (x - \alpha)(x - \beta) \) or \( (x - \alpha)(x - \gamma) \) or \( (x - \alpha)(x - \delta) \) but then the constant coefficient would be either \( \alpha \beta = i\sqrt{2} \) or \( \alpha \gamma = -\sqrt{2} \) or \( \alpha \delta = -i\sqrt{2} \), none of which is in \( L \).

(d) Show \( K = Q(\alpha, i) \).

**Solution:** As \( i = \beta/\alpha, i \in K \). Clearly \( \alpha \in K \). so \( Q(\alpha, i) \subset K \). But \( \alpha, \beta = i\alpha, \gamma = -\alpha, \delta = -i\alpha \) are all in \( Q(\alpha, i) \) so \( K \subset Q(\alpha, i) \).

(e) Show that \( [K : Q] = 8 \) and give a basis for \( K \) over \( Q \).

**Solution:** We get a tower \( Q \subset L \subset K \). \( [L : Q] = 2 \) with basis 1, \( i \). As \( K = L(\alpha) \) and \( \alpha \) satisfies an irreducible quartic in \( L[x] \), \( [K : L] = 4 \) with basis \( 1, \alpha, \alpha^2, \alpha^3 \). Thus \( [K : Q] = 8 \) with basic all products, namely \( 1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3 \).

(f) Show that \( |\Gamma| \leq 24 \). (This follows from general principles.)

**Solution:** Each \( \sigma \in \Gamma \) is determined by a permutation of \( \alpha, \beta, \gamma, \delta \) and there are only \( 4! = 24 \) such permutations.

(g) Show that actually \( |\Gamma| \leq 8 \). (Idea: \( \sigma(\alpha) \) determines \( \sigma(\gamma) \).)

**Solution:** There are four choice for \( \sigma(\alpha) \). But then \( \sigma(\gamma) = -\sigma(\alpha) \) is determined. Now there are two choices for \( \sigma(\beta) \) and then \( \sigma(\delta) \) is determined - giving 4 times 2 or 8 choices for \( \sigma \).

(h) List the eight possible permutations of \( \alpha, \beta, \gamma, \delta \) that could come from a \( \sigma \in \Gamma \).

**Solution:** We make a table:
(i) Actually $\Gamma$ is given by the eight permutations that you just found. Given this, show that $\Gamma$ is not Abelian.

**Solution:** Many of the pairs don’t commute, to show it isn’t Abelian we need only find one. For example, let $\sigma$ be given by row two and $\tau$ by row three. Then $(\sigma \tau)(\alpha) = \tau(\sigma(\alpha)) = \tau(\alpha) = \beta$ while $(\tau \sigma)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\beta) = \delta$ so $\sigma \tau \neq \tau \sigma$. 

<table>
<thead>
<tr>
<th>$\sigma(\alpha)$</th>
<th>$\sigma(\beta)$</th>
<th>$\sigma(\gamma)$</th>
<th>$\sigma(\delta)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha$</td>
<td>$\beta$</td>
<td>$\gamma$</td>
<td>$\delta$</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>$\delta$</td>
<td>$\gamma$</td>
<td>$\beta$</td>
</tr>
<tr>
<td>$\beta$</td>
<td>$\alpha$</td>
<td>$\delta$</td>
<td>$\gamma$</td>
</tr>
<tr>
<td>$\beta$</td>
<td>$\gamma$</td>
<td>$\delta$</td>
<td>$\alpha$</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>$\beta$</td>
<td>$\alpha$</td>
<td>$\delta$</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>$\delta$</td>
<td>$\alpha$</td>
<td>$\beta$</td>
</tr>
<tr>
<td>$\delta$</td>
<td>$\alpha$</td>
<td>$\beta$</td>
<td>$\gamma$</td>
</tr>
<tr>
<td>$\delta$</td>
<td>$\gamma$</td>
<td>$\beta$</td>
<td>$\alpha$</td>
</tr>
</tbody>
</table>