This note is about the subject of problems 5-8 in §12.2, the field
\[ E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, i) \].

We will see that it is the same as the field \( \mathbb{Q}(\zeta) \) where
\[ \zeta = \zeta_{24} = e^{2\pi i/24} = \cos(\pi/12) + i \sin(\pi/12), \]
a primitive 24th root of unity. This is an illustration of the theorem of Kronecker (not in the book) which says that every Galois extension of \( \mathbb{Q} \) with an Abelian Galois group (Abelian extension for short) is contained in a cyclotomic extension, i.e., one obtained by adjoining some root of unity. This is what I once called the “Sneakers Theorem.”

The degree \( [E : \mathbb{Q}] \) is 8 since we have
\[
\begin{array}{cccc}
K_0 & K_1 & K_2 & K_3 \\
\mathbb{Q} & \mathbb{Q}(\sqrt{2}) & \mathbb{Q}(\sqrt{2}, \sqrt{3}) & E
\end{array}
\]
and
\[ [E : \mathbb{Q}] = [E : K_2][K_2 : K_1][K_1 : \mathbb{Q}] = 2 \cdot 2 \cdot 2 = 8. \]
Thus the Galois group \( G = \text{Gal}(E/\mathbb{Q}) \) has order 8. A basis for \( E \) over \( \mathbb{Q} \) is
\[ \{1, \sqrt{2}, \sqrt{3}, i, \sqrt{-2}, \sqrt{-3}, i, \sqrt{-6}\} \].

In order to determine the lattice of intermediate fields, we need to know the lattice of subgroups of \( G \). According to Corollary 12.1.20, and element \( \phi \in G \) is determined by what it does to the field generators \( \sqrt{2}, \sqrt{3} \) and \( i \). Since each of them is the square root of a rational number, there is a Galois automorphism that sends it to its negative. Thus there are automorphisms \( g_1, g_2 \) and \( g_3 \) described by the following table.

<table>
<thead>
<tr>
<th>( \phi )</th>
<th>( \phi(\sqrt{2}) )</th>
<th>( \phi(\sqrt{3}) )</th>
<th>( \phi(i) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( g_1 )</td>
<td>-\sqrt{2}</td>
<td>\sqrt{3}</td>
<td>( i )</td>
</tr>
<tr>
<td>( g_2 )</td>
<td>\sqrt{2}</td>
<td>-\sqrt{3}</td>
<td>( i )</td>
</tr>
<tr>
<td>( g_3 )</td>
<td>\sqrt{2}</td>
<td>\sqrt{3}</td>
<td>(-i)</td>
</tr>
</tbody>
</table>

From this it is easy to deduce that \( g_1, g_2 \) and \( g_3 \) each have order 2 and that they commute with each other. This means that
\[ G \cong C_2 \times C_2 \times C_2 = \{1, g_1, g_2, g_3, g_1g_2, g_1g_3, g_2g_3, g_1g_2g_3\} \]

We need to work out the lattice of subgroups of \( G \). Since \( |G| = 8 \), its proper subgroups have order 2 and 4. Each of the 7 nontrivial elements of \( G \) has order 2 and thus generates a a subgroup of order 2.
Each subgroup of order 4 is generated by a pair of nontrivial elements, and there are 21 (or \( \binom{7}{2} \)) such pairs. However these 21 pairs do not determine 21 distinct subgroups. Consider the subgroup

\[ H = \langle x, y \rangle = \{1, x, y, z\} \quad \text{where} \quad z = xy. \]

Then

\[ H = \langle x, y \rangle = \langle x, z \rangle = \langle y, z \rangle. \]

This means the number of distinct subgroups of order 4 is \( \frac{1}{3} \) the number of pairs \( \{x, y\} \), or 7.

Each subgroup of order 4 has 3 subgroups of order 2, the ones generated by each of its 3 nontrivial elements.

A more subtle fact is that each subgroup of order 2 is contained in 3 subgroups of order 4. For a nontrivial element \( x \), the subgroup \( \langle x \rangle \) is contained in any subgroup of the form \( \langle x, y \rangle \). \( y \) could be any of the remaining 6 nontrivial elements, but since \( \langle x, y \rangle = \langle x, xy \rangle \), there are only 3 subgroups of order 4 containing \( \langle x \rangle \).

Here is a diagram of the lattice of subgroups.

(Note that this diagram is symmetric about the vertical axis. It took some experimenting to get it this way.)

Now we apply the Fundamental Theorem of Galois Theory to get the lattice of subfields. Each subgroup of order 4 has index 2 and therefore fixes a quadratic (degree 2) extension of \( \mathbb{Q} \). It turns out that the 7 basis elements other than 1 in (2) each generate one of these fields. To see this, consider the following table extending the one above.
Here the each sign indicates whether the indicated group element (in the left column) sends the indicated square roots to itself or to its negative. The bottom row indicates the subgroup fixing each of the 7 square roots. In each case it is generated by the elements corresponding any two of the plus signs in the column.

We can also use this table to read off the subfields fixed by subgroups of order two. These are indicated in the right column. In each case the subfield is generated by the square roots with pluses under them in the corresponding row.

It follows that the lattice of subfields is

Here the subgroup fixing each field is the one in the corresponding position in the subgroup diagram (3). As usual, the arrows here go in the opposite direction from the ones in (3).
Now we will discuss the relation between our field $E$ and the cyclotomic field $\mathbb{Q}(\zeta_{24})$, where $\zeta_{24}$ is as in (1). For a positive integer $n$, let

$$\zeta_n = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}),$$

the standard primitive $n$th root of unity. Observe that

$$\zeta_6 = \frac{1 + \sqrt{-3}}{2} \quad \text{so} \quad \mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3}),$$

and

$$\zeta_4 = \omega = i \quad \text{so} \quad \mathbb{Q}(\zeta_4) = \mathbb{Q}(i).$$

Hence, since $\zeta_{12} = \zeta_3/\zeta_4$, it follows that

$$\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\sqrt{-3}, i) = \mathbb{Q}(\sqrt{3}, i).$$

We also have

$$\zeta_8 = \frac{1 + i}{\sqrt{2}} \quad \text{so} \quad \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i).$$

Then since $\zeta_{24} = \zeta_8/\zeta_{12}$, it follows that

$$\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, i) = E$$
as claimed above.

We will now analyze the Galois group of this field in terms of $\zeta$. First we need to find its minimal polynomial. We have

$$x^{24} - 1 = (x^{12} - 1)(x^{12} + 1) = (x^8 + x^4 + 1)(x^8 - 1)(x^4 - 1)(x^8 - x^4 + 1)(x^4 + 1) = (x^8 + x^4 + 1)(x^8 - 1)(x^8 - x^4 + 1).$$

Now any zero of the first factor is a 12th root of unity, and any zero of the second is an 8th root. Hence the primitive 24 roots are all zeros of the third one, which is the minimal polynomial $f(x)$.

$$f(x) = x^8 - x^4 + 1 = (x - \zeta)(x - \zeta^5)(x - \zeta^7)(x - \zeta^{11})(x - \zeta^{13})(x - \zeta^{17})(x - \zeta^{19})(x - \zeta^{23})$$

Since $F(\zeta) = 0$, $\zeta^8 = \zeta^4 - 1$ and

$$\begin{align*}
\zeta^9 &= \zeta^5 - \zeta \\
\zeta^{10} &= \zeta^6 - \zeta^2 \\
\zeta^{11} &= \zeta^7 - \zeta^3 \\
\zeta^{12} &= \zeta^8 - \zeta^4 = -1 \\
\zeta^{k+12} &= -\zeta^k \quad \text{for } 0 < k < 12
\end{align*}$$

A Galois automorphism $\phi$ is determined by what it does to $\zeta$, and $\phi(\zeta)$ must be another primitive 24th root of unity. Let $g_k$ denote the automorphism that sends $\zeta$ to $\zeta^k$ for $k = 5, 7, 11, 13, 17, 19$ or $23$. One can check that each of these has order two. This is related to the arithmetic fact that if $k$ is an integer not divisible by 2 or 3, then $k^2 - 1$ is a multiple of 24.
Since
\[
g_{11} = g_5g_7 \\
g_{17} = g_5g_{13} \\
g_{19} = g_7g_{13} \\
g_{23} = g_9g_{13},
\]
the group is generated by \(g_5\), \(g_7\) and \(g_{13}\). We need to express these in terms of \(g_1\), \(g_2\) and \(g_3\) above. We have
\[
\begin{align*}
\zeta^4 = \zeta_8 &= \frac{1 + i}{\sqrt{2}} = \frac{1 + \zeta^6}{\sqrt{2}} \\
\sqrt{2} &= \frac{1 + \zeta^6}{\zeta^4} = \zeta^3 + \zeta^{-3} \\
\zeta^4 = \zeta_6 &= \frac{1 + \sqrt{-3}}{2} \\
\sqrt{-3} &= 2\zeta^4 - 1 \\
\sqrt{3} &= \zeta^6(2\zeta^4 - 1) = 2\zeta^{10} - \zeta^6 \\
&= 2(\zeta^6 - \zeta^2) - \zeta^6 = \zeta^6 - 2\zeta^2 \\
i &= \zeta^6
\end{align*}
\]
From these we can deduce the following table.
\[
\begin{array}{cccc}
g & \phi(\sqrt{2}) & \phi(\sqrt{3}) & \phi(i) \\
g_5 & -\sqrt{2} & -\sqrt{3} & i \\
g_7 & \sqrt{2} & -\sqrt{3} & -i \\
g_{13} & -\sqrt{2} & \sqrt{3} & i \\
\end{array}
\]
This means
\[
g_5 = g_1g_2 \\
g_7 = g_2g_3 \\
g_{13} = g_1
\]