1. Page 560, number 4: (20 points) set $E = Q(\sqrt{2}, \sqrt{5}, \sqrt{7})$. Then $E$ is a splitting field of $(x^2 - 2)(x^2 - 5)(x^2 - 7)$ over $Q$. By the Fundamental Theorem of Galois Theory $K \mapsto Gal(E/Q)$ describes a bijective correspondence between the subfields of $F$ which contain $Q$ (any subfield of $E$ must contain $Q$) and $[K : Q] = [Gal(E/Q) : Gal(E/K)]$. Since $|Gal(E/Q)| = 8$ we conclude that $4 = [K : Q]$ if and only if $|Gal(K/Q)| = 2$ (10).

We are given that $Gal(E/Q) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Writing $G = Gal(E/Q)$ in multiplicative notation we have $a^2 = e$ for all $a \in G$. Therefore there are 7 subgroups of $G$ of order 2 which means there are 7 subfields of $E$ of degree 4 over $Q$ (10).


Note 2 = $[Q(\sqrt{10}) : Q]$ since $\sqrt{10}$ is a root of $x^2 - 10 \in Q[x]$ which is irreducible by the Eisenstein Criterion with $p = 2$ or $p = 5$ (5). Therefore $2 = [Q(\sqrt{10}) : Q] = |Gal(Q(\sqrt{10})/Q)|$ by the Fundamental Theorem of Galois Theory (5).

3. Page 561, number 12: (40 points) $x^3 - 1 = (x - 1)(x^2 + x + 1)$. Let 

$$\omega = e^{2\pi i/3} = \cos\left(\frac{2\pi i}{3}\right) + i\sin\left(\frac{2\pi i}{3}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

be a primitive 3rd root of unity. Then $x^3 - 1 = (x - 1)(x - \omega)(x - \omega^2)$ which means that $Q(\omega)$ is a splitting field of $x^3 - 1$ over $Q$ and $\omega$ is a root of $(x - \omega)(x - \omega^2) = x^2 + x + 1 \in Q[x]$. The latter implies that $[Q(\omega) : Q] \leq 2$. Since $\omega \not\in R$ it follows that $[Q(\omega) : Q] = 2$ (5).

Let $E = Q(\omega)$. By definition $Gal(E/F)$ is the Galois group of $x^3 - 1$ over $Q$. By the Fundamental Theorem of Galois Theory $|Gal(E/Q)| = [E : Q] = 2$ which means $Gal(E/Q) \cong \mathbb{Z}_2$ (5).

Observe that $x^3 - 2 = (x - 2^{1/3})(x - \omega 2^{1/3})(x - \omega^2 2^{1/3})$. Therefore a splitting field of $x^3 - 2$ over $Q$ is $E = Q(2^{1/3}, \omega 2^{1/3}, \omega^2 2^{1/3}) = Q(2^{1/3}, \omega)$. The last equation holds since $\omega = \omega(2^{1/3})^{-1} \in E$. By definition the Galois group of $x^3 - 2$ over $Q$ is $Gal(E/Q)$.

We have shown that $[Q(\omega) : Q] = 2$. Now $[Q(2^{1/3}) : Q] = 3$ since $2^{1/3}$ is a root of $x^3 - 2 \in Q[x]$ and the latter is irreducible by the Eisenstein Criteron with $p = 2$. Therefore $[E : Q] = [Q(\omega, 2^{1/3}) : Q] = 6$ by (D). By the Fundamental Theorem of Galois Theory $|Gal(E/Q)| = [E : Q] = 6$ (5).

Let $\sigma \in Gal(E/Q)$. Then $\sigma(2^{1/3}) \in \{2^{1/3}, \omega 2^{1/3}, \omega^2 2^{1/3}\} = R_1$, the set of roots of $x^3 - 2$ in $E$, by (A). Likewise $\sigma(\omega) \in \{\omega, \omega^2\} = R_2$, the set of roots of $x^2 + x + 1$ in $E$. Thus there are $|R_1||R_2| = 3 \times 2 = 6$ possible choices for the pair $(\sigma(2^{1/3}), \sigma(\omega))$. Since $Gal(E/Q) = 6$, given $r_1 \in R_1$ and $r_2 \in R_2$ there exists a $\sigma \in Gal(E/Q)$ such that $\sigma(2^{1/3}) = r_1$ and $\sigma(\omega) = r_2$ by (B).

Let $\tau, \sigma \in Gal(E/Q)$ satisfy 

$$\tau(\omega) = \omega^2$$

and 

$$\tau(2^{1/3}) = 2^{1/3}$$

(5)
and
\[ \sigma(\omega) = \omega \text{ and } \sigma(2^{1/3}) = \omega 2^{1/3} \quad (5). \]

Then \( \tau, \sigma \neq \text{Id} \). Note
\[ \tau^2(\omega) = \tau(\tau(\omega)) = \tau(\omega^2) = \tau(\omega)^2 = (\omega^2)^2 = \omega^4 = \omega, \]
as \( \omega^3 = 1 \), and
\[ \tau^2(2^{1/3}) = \tau(\tau(2^{1/3})) = \tau(2^{1/3}) = 2^{1/3}. \]

Therefore \( \tau^2 = \text{Id} \) by (B) which means \( \tau \) has order 2.

Likewise
\[ \sigma^3(\omega) = \omega \]
and, since by induction \( \sigma^n(2^{1/3}) = \omega^n2^{1/3} \) for all \( n \geq 0 \), we have
\[ \sigma^3(2^{1/3}) = \omega^32^{1/3} = 2^{1/3}. \]

Therefore \( \sigma^3 = \text{Id} \) by (B) again and thus has order 3. Since \( \tau^{-1} = \tau \),
\[ \tau \sigma \tau^{-1}(\omega) = \tau(\sigma(\tau(\omega))) = \tau(\sigma(\omega^2)) = \tau(\sigma(\omega)^2) = \tau(\omega^2) = \tau(\omega)^2 = (\omega^2)^2 = \omega^4 = \omega = \sigma^{-1}(\omega), \]
as \( \sigma(\omega) = \omega \) implies \( \omega = \sigma^{-1}(\omega) \), and
\[ \tau \sigma \tau^{-1}(2^{1/3}) = \tau(\sigma(\tau(2^{1/3}))) = \tau(\sigma(2^{1/3})) = \tau(\omega 2^{1/3}) = \tau(\omega) \tau(2^{1/3}) = \omega^22^{1/3} = \sigma^2(2^{1/3}). \]

Therefore \( \tau \sigma \tau^{-1} = \sigma^2 \) by (B) again, and thus \( \tau \sigma \tau^{-1} = \sigma^{-1} \) as \( \sigma \) has order 3 (5). Thus \( \text{Gal}(E/Q) \simeq D_3 (5) \).

4. Page 561, number 16: (20 points) By the Fundamental Theorem of Galois Theory \( |\text{Gal}(E/F)| = [E : F] \) is finite and the subgroups of \( G = \text{Gal}(E/F) \) are in one-one correspondence with the subfields of \( E \) which contain \( F \) (10). Since \( G \) is finite it has only finitely subgroups; thus \( E \) has only finitely many subfields \( K \) which contain \( F \) (10).