Solutions to Homework 8

Problem 1. Cox, Section 6.1, Exercise 2, variant:
Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, let $K_2 = \mathbb{Q}(\sqrt{2})/\mathbb{Q}$, and let $K_3 = \mathbb{Q}(\sqrt{3})/\mathbb{Q}$, so that $L/K_i/\mathbb{Q}$ for $i = 1, 2$.

(a) Apply Proposition 5.1.8 to L/K_3 to show that there is some $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$.

(b) Apply Proposition 5.1.8 to L/K_2 to show that there is some $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\tau(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{3}) = -\sqrt{3}$.

(c) Combine parts (a) and (b) with Example 6.1.10 to prove that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. We know from past examples that $[L : \mathbb{Q}] = 4$, and hence $[L : K_i] = 2$ for each $i = 2, 3$. We also know that L is the splitting field of $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$.

(a) Let $f_2 = x^2 - 2$, which is irreducible over K_3 since $\deg f_2 = 2$ and $\pm\sqrt{2} \notin K_3$.
The two roots of f_2 in L are $\pm\sqrt{2}$. By Proposition 5.1.8, there exists some $\sigma \in \mathrm{Gal}(L/K_3)$ such that $\sigma(\sqrt{2}) = -\sqrt{2}$.
Thus, σ is also an element of $\mathrm{Gal}(L/\mathbb{Q})$, being an automorphism of L that fixes every element of $K_3 \supseteq \mathbb{Q}$, and hence $\sigma(\sqrt{3}) = \sqrt{3}$, since $\sqrt{3} \in K_3$. QED (a)

(b) Let $f_3 = x^2 - 3$, which is irreducible over K_2 since $\deg f_3 = 2$ and $\pm\sqrt{3} \notin K_2$.
The two roots of f_3 in L are $\pm\sqrt{3}$. By Proposition 5.1.8, there exists some $\tau \in \mathrm{Gal}(L/K_2)$ such that $\sigma(\sqrt{3}) = -\sqrt{3}$.
Thus, τ is also an element of $\mathrm{Gal}(L/\mathbb{Q})$, being an automorphism of L that fixes every element of $K_2 \supseteq \mathbb{Q}$, and hence $\tau(\sqrt{2}) = \sqrt{2}$, since $\sqrt{2} \in K_2$. QED (b)

(c) By Example 6.1.10, we know that $|\mathrm{Gal}(L/\mathbb{Q})| \leq 4$, and that any element of $\mathrm{Gal}(L/\mathbb{Q})$ is determined by its values at $\sqrt{2}$ and at $\sqrt{3}$. (Which must be $\pm\sqrt{2}$ and $\pm\sqrt{3}$, respectively.)
By parts (a), (b), we have $\mathrm{id}_L, \sigma, \tau, \sigma\tau \in \mathrm{Gal}(L/\mathbb{Q})$.
These four automorphisms are indeed all different, since σ and id_L both fix $\sqrt{3}$ while τ and $\sigma\tau$ do not; and τ and id_L both fix $\sqrt{2}$ while σ and $\sigma\tau$ do not. Therefore, $\mathrm{Gal}(L/\mathbb{Q}) = \{\mathrm{id}_L, \sigma, \tau, \sigma\tau\}$.
Observe that σ has order 2, since $\sigma(\sqrt{2}) \neq \sqrt{2}$, but $\sigma^2(\sqrt{2}) = \sqrt{2}$ and $\sigma^2(\sqrt{3}) = \sqrt{3}$, so that $\sigma^2 = \mathrm{id}_L$.
Similarly τ has order 2. Finally, $\sigma\tau$ sends both $\sqrt{2}$ to $-\sqrt{2}$ and $\sqrt{3}$ to $-\sqrt{3}$, so that $(\sigma\tau)^2$ fixes both $\sqrt{2}$ and $\sqrt{3}$. By Example 6.1.10 (which in turn is by Proposition 6.1.4), it follows that $(\sigma\tau)^2 = e$.
This is precisely the multiplication table for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. QED (c)

Sketch of Alternative Proof of (c): After observing $\mathrm{Gal}(L/\mathbb{Q}) = \{\mathrm{id}_L, \sigma, \tau, \sigma\tau\}$ by the same reasoning as above, define $\phi : \mathrm{Gal}(L/\mathbb{Q}) \to \{\pm 1\} \times \{\pm 1\}$ by $\phi(\lambda) = \left(\frac{\lambda(\sqrt{2})}{\sqrt{2}}, \frac{\lambda(\sqrt{3})}{\sqrt{3}}\right)$. It is easy to prove that ϕ is a homomorphism. Then one can check that ϕ is onto by applying ϕ to each of $\mathrm{id}_L, \sigma, \tau, \sigma\tau \in \mathrm{Gal}(L/\mathbb{Q})$. Finally, since $|\mathrm{Gal}(L/\mathbb{Q})| = 4$, we get that ϕ is also one-to-one, by the pigeonhole principle. Thus, ϕ is an isomorphism.

Note: Since this problem set extends into Section 6.2, then even though this problem came from Section 6.1, I'm OK with you quoting Theorem 6.2.1 rather than Example 6.1.10, as follows:
We know that $L/\mathbb{Q}$ is the splitting field of $(x^2 - 2)(x^2 - 3)$ and hence is normal. We know that $L/\mathbb{Q}$ is separable since $\mathrm{char}\,\mathbb{Q} = 0$. Therefore, by Theorem 6.2.1, we have $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 4$.

Problem 2. Cox, Section 6.1, Exercises 5–6, variant:
Let $m_1, \ldots, m_n \in \mathbb{Z}$ be pairwise relatively prime squarefree integers, none of which is 1. [That is, no m_i is 1 or is divisible by the square of any prime, and for all $i \neq j$, we have $\gcd(m_i, m_j) = 1$.]

(a) Prove that $\sqrt{m_n} \notin \mathbb{Q}\big(\sqrt{m_1}, \ldots, \sqrt{m_{n-1}}\big)$. [**Suggestion**: Induction on n.]

(b) Use Theorem 6.2.1 to prove that $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{m_1},\ldots,\sqrt{m_n}\right)/\mathbb{Q}\right)$ has order 2^n.

(c) Prove that $\left|\,\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{6},\sqrt{10},\sqrt{15}\right)/\mathbb{Q}\right)\right| = 4$.

[**Note**: Using the ideas of Problem 1, can you prove that $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{m_1},\ldots,\sqrt{m_n}\right)/\mathbb{Q}\right) \cong (\mathbb{Z}/2\mathbb{Z})^n$?]

Proof. (a) We proceed by induction on $n \geq 1$.

Base case: For $n = 1$, the hypotheses say that m_1 is not a square in $\mathbb{Z}$, i.e., $x^2 - m_1$ has no roots in $\mathbb{Z}$. By Gauss's Lemma, then, the same polynomial has no roots in $\mathbb{Q}$. Thus, $\sqrt{m_1} \notin \mathbb{Q}$.
[**Note**: Or you can just say, "We know $\sqrt{m_1} \notin \mathbb{Q}$" without mentioning Gauss's Lemma and all that other nonsense.]

Inductive Step: Given $n \geq 2$, assume the statement holds for $n-1$. Let $K = \mathbb{Q}(\sqrt{m_1},\ldots,\sqrt{m_{n-2}})$ and $L = \mathbb{Q}(\sqrt{m_1},\ldots,\sqrt{m_{n-1}})$, so that $L = K(\sqrt{m_{n-1}})$.
Suppose $\sqrt{m_n} \in L$. Then we may write $\sqrt{m_n} = a + b\sqrt{m_{n-1}}$ with $a, b \in K$. We consider three cases.

If $b = 0$, then $\sqrt{m_n} = a \in K$, contradicting the inductive hypothesis, since $\{m_1,\ldots,m_{n-2}\} \cup \{m_n\}$ is a set of $n-1$ pairwise relatively prime squarefree integers, none of which is 1.

If $a = 0$, then $\sqrt{m_{n-1}m_n} = bm_{n-1} \in K$, again contradicting the inductive hypothesis, since $\{m_1,\ldots,m_{n-2}\} \cup \{m_{n-1}\cdot m_n\}$ is a set of $n-1$ pairwise relatively prime squarefree integers, none of which is 1.

Finally, if $a, b \neq 0$, then $m_n = a^2 + b^2 m_{n-1} + 2ab\sqrt{m_{n-1}}$, so $\sqrt{m_{n-1}} = (2ab)^{-1}(m_n - a^2 - b^2 m_{n-1}) \in K$, again contradicting the inductive hypothesis. QED (a)

(b) For each $i = 0,\ldots,n$, let $K_i = \mathbb{Q}(\sqrt{m_1},\ldots,\sqrt{m_i}) = K_{i-1}(\sqrt{m_i})$. By part (a), we have $\sqrt{m_i} \notin K_{i-1}$, and hence the quadratic polynomial $x^2 - m_i$ is irreducible over K_{i-1}. Therefore, we have $[K_i : K_{i-1}] = 2$. By the Tower Theorem,

$$[K_n : \mathbb{Q}] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}]\cdots[K_1 : K_0] = 2^n.$$

Note $K_n = \mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_n})$ is the splitting field of the separable polynomial $(x^2 - p_1)\cdots(x^2 - p_n)$. Hence, by Theorem 6.2.1, we have $|\,\mathrm{Gal}(K_n/\mathbb{Q})| = [K_n : \mathbb{Q}] = 2^n$. QED (b)

(c) Let $K = \mathbb{Q}\left(\sqrt{6},\sqrt{10}\right)$ and $L = K\left(\sqrt{15}\right) = \mathbb{Q}\left(\sqrt{6},\sqrt{10},\sqrt{15}\right)$.
Note that $\sqrt{15} = \dfrac{1}{4}\sqrt{60} = \dfrac{1}{4}\sqrt{6}\sqrt{10} \in K$. Thus, $L = K\left(\sqrt{15}\right) = K$.
Let $E = \mathbb{Q}(\sqrt{6})$, so that $[E : \mathbb{Q}] = 2$. Then since $\sqrt{10}$ is a root of $f(x) = x^2 - 10 \in E[x]$, and since $K = E(\sqrt{10})$, we have that $[K : E] \leq \deg f = 2$.
Therefore, $[L : \mathbb{Q}] = [K : \mathbb{Q}] = [K : E][E : \mathbb{Q}] \leq 2 \cdot 2 = 4$. QED (c)

Problem 3. Cox, Section 6.2, Exercise 3:
Let $L = \mathbb{Q}(\zeta_5, \sqrt[5]{2})$. Recall that the minimal polynomial of ζ_5 over $\mathbb{Q}$ is $\Phi_5 = x^4 + x^3 + x^2 + x + 1$.

(a) Prove that $[L : \mathbb{Q}] = 20$.

(b) Prove that L is the splitting field of $x^5 - 2$ over $\mathbb{Q}$, and conclude (by Theorem 6.2.1) that $|\,\mathrm{Gal}(L/\mathbb{Q})| = 20$.

Proof. (a) Let $E = \mathbb{Q}(\zeta_5)$ and $K = \mathbb{Q}(\sqrt[5]{2})$.
Since Φ_5 is the minimal polynomial of ζ_5 over $\mathbb{Q}$, we have $[E : \mathbb{Q}] = \deg \Phi_5 = 4$ Since $f(x) = x^5 - 2$ has $\sqrt[5]{2}$ as a root, it follows that $[L : E] = [E(\sqrt[5]{2}) : E] \leq 5$.
Thus, $[L : \mathbb{Q}] = [L : E][E : \mathbb{Q}] \leq 20$ is divisible by 4.
Since f is the minimal polynomial of $\sqrt[5]{2}$ over $\mathbb{Q}$ (it is irreducible by Eisenstein with $p = 2$), we have $[K : \mathbb{Q}] = \deg f = 5$. Thus, $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}]$ is divisible by 5.
Being a positive integer at most 20 and divisible by both 4 and 5, it follows that $[L : \mathbb{Q}] = 20$. QED (a)

(b) The roots of $f = x^5 - 2$ are $\zeta_5^j \sqrt[5]{2}$ for $j = 0, 1, 2, 3, 4$, which are all distinct since $\zeta_5^i \neq 1$ for $1 \leq i \leq 4$.
All five roots are clearly in $L = \mathbb{Q}(\zeta_5, \sqrt[5]{2})$, so L contains a splitting field M of f.

Conversely, $\sqrt[5]{2} \in M$, and $\zeta_5 = (\zeta_5 \sqrt[5]{2})/\sqrt[5]{2} \in M$. Thus, $L \subseteq M$, so $L = M$ is the splitting field of f over $\mathbb{Q}$. By Theorem 6.2.1, then, $|\operatorname{Gal}(L/\mathbb{Q})| = 20$. QED (b)

Problem 4. Cox, Section 6.2, Exercise 5:
Let $\operatorname{char} F = p$, and suppose $f = x^p - x + a \in F[x]$ is irreducible over F. Let $L = F(\alpha)$, where α is a root of f; in Exercise 5.3.16 (Homework 7, Problem 6), you showed that L/F is normal and separable.

(a) Prove $|\operatorname{Gal}(L/F)| = p$. [Of course, it follows that $\operatorname{Gal}(L/F) \cong \mathbb{Z}/p\mathbb{Z}$, by Lagrange.]

(b) Recall from Exercise 5.3.16 that $\alpha + 1$ is a root of f. For each $i = 0, \ldots, p-1$, prove that there is a unique element of $\operatorname{Gal}(L/F)$ that takes α to $\alpha + i$.

(c) Find an explicit isomorphism $\operatorname{Gal}(L/F) \cong \mathbb{Z}/p\mathbb{Z}$. [And justify your claims, of course.]

Proof. (a) By the assumption that f is irreducible over F, we have $[L : F] = [F(\alpha) : F] = \deg(f) = p$. As noted in the statement of the problem, we know from Exercise 5.3.16 that L/F is normal and separable. Therefore, by Theorem 6.2.1, we have $|\operatorname{Gal}(L/F)| = [L : F] = p$. QED (a)

(b) Observe that for any integer $i \in \mathbb{Z}$, we have that $\alpha + i$ is also a root of f. This can be proven by induction using the fact about $\alpha + 1$ mentioned in the statement of the problem, or by computing:

$$f(\alpha + i) = (\alpha + i)^p - (\alpha + i) + a = (\alpha^p - \alpha + a) + (i^p - i) = f(\alpha) + 0 = 0,$$

since Fermat's Little Theorem yields $i^p = i$ in the field F, since $i \in \mathbb{Z}$ and $\operatorname{char} F = p$.

By Proposition 5.1.8, for each $i \in \mathbb{Z}$, there is some $\sigma_i \in \operatorname{Gal}(L/F)$ such that $\sigma_i(\alpha) = \alpha + i$.

In addition, the integers $0, 1, \ldots, p-1$ are all distinct in F, since p is the *smallest* positive integer that is zero in F. Thus, the elements $\alpha + 0, \alpha + 1, \ldots, \alpha + (p-1)$ are all distinct in F, and hence the maps $\sigma_0, \sigma_1, \ldots, \sigma_{p-1}$ are all distinct as well.

By part (a), then, $\sigma_0, \sigma_1, \ldots, \sigma_{p-1}$ must be all p elements of $\operatorname{Gal}(L/F)$. Therefore, for each $i = 0, 1, \ldots, p-1$, there is one and only one map in $\operatorname{Gal}(L/F)$ that takes α to $\alpha + i$, namely σ_i. QED (b)

(c) Define $\phi : \mathbb{Z} \to \operatorname{Gal}(L/F)$ by $\phi(i) = \sigma_i$. Since part (b) gives us $\operatorname{Gal}(L/F) = \{\sigma_0, \sigma_1, \ldots, \sigma_{p-1}\}$, it is immediate that ϕ is surjective. To see that ϕ is a group homomorphism, given $i, j \in \mathbb{Z}$, we have

$$\sigma_{i+j}(\alpha) = \alpha + (i + j) = (\alpha + j) + i = \sigma_i(\alpha + j) = \sigma_i(\sigma_j(\alpha)).$$

Since any $\tau \in \operatorname{Gal}(L/F)$ is determined by $\tau(\alpha)$, it follows that

$$\phi(i + j) = \sigma_{i+j} = \sigma_i \circ \sigma_j = \phi(i) \circ \phi(j),$$

as desired. Finally, we claim that $\ker(\phi) = p\mathbb{Z}$:

($\subseteq$): Given $i \in \ker(\phi)$, we have $\sigma_i(\alpha) = \alpha$, whence $\alpha + i = \alpha$ and hence $i = 0$ in F. Since $\operatorname{char} F = p$, this means $p | i$ in $\mathbb{Z}$, so $i \in p\mathbb{Z}$.
($\supseteq$): Given $i \in p\mathbb{Z}$, we have $i = 0$ in F, and hence $\sigma_i(\alpha) = \alpha + i = \alpha$. Since $L = F(\alpha)$, Proposition 6.1.4(b) again yields $\sigma_i = \mathrm{id}_L$, so $i \in \ker(\phi)$, proving the claim.

By the Fundamental Theorem of Group Homomorphisms, then, the map $\bar{\phi} : \mathbb{Z}/p\mathbb{Z} \to \operatorname{Gal}(L/F)$ by $\bar{\phi}(i + p\mathbb{Z}) = \sigma_i$ is an isomorphism of groups. Thus, the isomorphism requested in the problem is $\bar{\phi}^{-1}$, given by

$$\sigma_i \mapsto i + p\mathbb{Z} \quad \text{for all } i = 0, 1, \ldots, p-1.$$ QED (c)

Problem 5. Cox, Section 6.2, Exercise 6: Let $f \in F[x]$ be irreducible and separable of degree $n \geq 1$, and let L/F be the splitting field of f over F. Prove that n divides $|\operatorname{Gal}(L/F)|$.

Proof. Let $\alpha \in L$ be a root of f, which exists since L is a splitting field of f and $\deg f \geq 1$. Define $K = F(\alpha)$, so that $L/K/F$.
Since f is irreducible over F, we have $[K : F] = \deg f = n$. Therefore, by Theorem 6.2.1 and the Tower Theorem, $|\operatorname{Gal}(L/F)| = [L : F] = [L : K][K : F] = [L : K]n$ is divisible by n. QED

Problem 6. Cox, Section 6.3, Exercise 2, variant:

For each of the following Galois groups, find an explicit subgroup of S_4 that it is isomorphic to, in that it permutes the roots of the given quartic polynomial according to that subgroup of S_4. [Of course, justify your answers.]

(a) $\mathrm{Gal}(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q})$, viewing $\mathbb{Q}(i,\sqrt{2})$ as the splitting field of $f = x^4 - 4$ over $\mathbb{Q}$.

(b) $\mathrm{Gal}(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q})$, viewing $\mathbb{Q}(i,\sqrt{2})$ as the splitting field of $g = x^4 - 2$ over $\mathbb{Q}$.

Solution/Proof. (a) Let $L = \mathbb{Q}(i,\sqrt{2})$ and $G = \mathrm{Gal}(L/\mathbb{Q})$. By Problem 2(b) (Cox 6.1 #5) with $m_1 = -1$ and $m_2 = 2$, we have $[L:\mathbb{Q}] = 4$, and hence $|G| = 4$ by Theorem 6.2.1.
The polynomial $f = x^4 - 4$ factors over $\mathbb{Q}$ as $f = f_1 f_2$ where $f_1 = x^2 - 2$ and $f_2 = x^2 + 2$, where f_1 has roots $\pm\sqrt{2}$ and f_2 has roots $\pm\sqrt{-2}$.
Any automorphism of L fixing $\mathbb{Q}$ must permute the roots of f_1 while separately permuting the roots of f_2. Therefore, indexing the roots of f_1 as 1 and 2, and indexing the roots of f_2 as 3 and 4, any $\sigma \in G$ must act on $\{1,2,3,4\}$ as an element of

$$H = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \subseteq S_4$$

That is, G is isomorphic to a subgroup of H. But since $|H| = 4 = |G|$, it follows that $G \cong H$. QED (a)

(b) Let $L = \mathbb{Q}(i,\sqrt[4]{2})$ and $G = \mathrm{Gal}(L/\mathbb{Q})$. We saw in Homework 4, Problem 6(a) (Cox 4.3 #2(a)) that $[L:\mathbb{Q}] = 8$. We also have that L is the splitting field of g over $\mathbb{Q}$ (since the roots of g are $i^j\sqrt[4]{2}$ for $j = 0,1,2,3$). Thus, by Theorem 6.2.1, $|G| = [L:\mathbb{Q}] = 8$.
Any $\sigma \in G$ is determined by the values of $\sigma(\sqrt[4]{2})$ and $\sigma(i)$. [This is because L is obtained from $\mathbb{Q}$ by adjoining $\sqrt[4]{2}$ and i.] Such σ must map i to either i or $-i$ (the two roots of $h = x^2 + 1 \in \mathbb{Q}[x]$), and it must map $\sqrt[4]{2}$ to one of the four roots of g. Since there are only $2 \cdot 4 = 8$ such choices of how to do this, each such combination must be attained by exactly one $\sigma \in G$.
The four roots of g are $i^j\sqrt[4]{2}$ for $j = 0,1,2,3$. Thus, each $\sigma \in G$ is uniquely determined by a pair of integers $(k,\ell) \in \{0,1\} \times \{0,1,2,3\}$, where $\sigma(i) = (-1)^k i$ and $\sigma(\sqrt[4]{2}) = i^\ell\sqrt[4]{2}$.
For $\sigma \in G$ with $k = 0$, i.e., for which $\sigma(i) = i$, we have

$$\sigma(i^j\sqrt[4]{2}) = i^j\sigma(\sqrt[4]{2}) = i^{j+\ell}\sqrt[4]{2}.$$

For $\sigma \in G$ with $k = 1$, i.e., for which $\sigma(i) = -i$, we have

$$\sigma(i^j\sqrt[4]{2}) = (-i)^j\sigma(\sqrt[4]{2}) = i^{-j+\ell}\sqrt[4]{2}.$$

Index the roots $i^j\sqrt[4]{2}$ of g from 1 to 4 by $j+1$, i.e., $\sqrt[4]{2}$ is root number 1, $i\sqrt[4]{2}$ is root number 2, and so on. For $\sigma \in G$ with $k = 0$ and $\ell = 1$, then, the formulas above show that σ permutes these roots as the 4-cycle (1 2 3 4). The other elements of G with $k = 0$ are σ^ℓ for $\ell = 0,2,3$, namely e, (1 3)(2 4), and (1 4 3 2). Note that $\langle\sigma\rangle$ forms a cyclic subgroup of G.
For $\tau \in G$ with $k = 1$ and $\ell = 0$, the formulas above show that τ permutes the roots as (2 4). Thus, the other four elements of G must be the elements of the coset $\langle\sigma\rangle\tau = \{\sigma^\ell\tau \,|\, 0 \le \ell \le 3\}$.
Thus, $G = \{\sigma^\ell\tau^k | k \in \{0,2\}, \ell \in \{0,1,2,3\}\}$ is isomorphic to the dihedral group D_4, represented explicitly in S_4 as the subgroup

$$H = \{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (2\ 4), (1\ 2)(3\ 4), (1\ 3), (1\ 4)(2\ 3)\} \subseteq S_4.$$

QED (b)

Problem 7. Cox, Section 6.3, Exercise 4:
Let $\alpha = \sqrt{2+\sqrt{2}}$, and let $L = \mathbb{Q}(\alpha)$. In Exercise 5.1.6 (Homework 5, Problem 7), you showed that $f = x^4 - 4x^2 - 2$ is the minimal polynomial of α over $\mathbb{Q}$, with splitting field L. Prove that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

Proof. Since $L = \mathbb{Q}(\alpha)$ and f is irreducible over $\mathbb{Q}$, we have $[L:\mathbb{Q}] = \deg f = 4$.
As noted in the statement of the problem, Exercise 5.1.6 told us that L is a splitting field over $\mathbb{Q}$, and hence $L/\mathbb{Q}$ is normal. This extension is also separable since $\mathrm{char}\,\mathbb{Q} = 0$. Therefore, by Theorem 6.2.1, we have $|\,\mathrm{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 4$.
We saw in Exercise 5.1.6 that the four roots of f are $\pm\alpha$ and $\pm\beta$, where $\beta = \sqrt{2-\sqrt{2}}$. We also saw that $\beta = (\alpha^2 - 2)/\alpha$, and that $\alpha\beta = \sqrt{2}$.

By Theorem 6.1.4, there exists $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\alpha) = \beta$. Therefore,

$$\sigma(\beta) = \sigma\left(\frac{\alpha^2 - 2}{\alpha}\right) = \frac{\beta^2 - 2}{\beta} = \frac{(2 - \sqrt{2}) - 2}{\beta} = -\frac{\sqrt{2}}{\beta} = -\alpha,$$

where the last equality is because $\alpha\beta = \sqrt{2}$. Thus, $\sigma(\alpha) = \beta \neq \alpha$, and $\sigma^2(\alpha) = -\alpha \neq \alpha$. It follows that the order of σ, denoted $o(\sigma)$, is neither 1 nor 2.

On the other hand, since $|\mathrm{Gal}(L/F)| = 4$, we have $o(\sigma)|4$, by Lagrange's Theorem. Since $o(\sigma) \neq 1, 2$, we must have $o(\sigma) = 4$. Because $|\mathrm{Gal}(L/F)| = 4$, it follows that $\mathrm{Gal}(L/F)$ is cyclic (with generator σ), and hence $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. QED

Problem 8. Cox, Section 6.4, Exercise 7:
Prove that S_n is generated by the transposition $\tau = (1\ 2)$ and the n-cycle $\sigma = (1\ 2\ \ldots\ n)$

Proof. Let H be the subgroup of S_n generated by $\tau = (1, 2)$ and $\sigma = (1, 2, \ldots, n)$. First, observe that for each index $j = 1, \ldots, n-1$, we have $\sigma^{j-1}(1) = j$, and $\sigma^{j-1}(2) = j + 1$. Thus,

$$(j, j+1) = \sigma^{j-1}\tau\sigma^{-j+1} \in H \quad \text{for every } j = 1, 2, \ldots, n-1. \tag{1}$$

Second, we claim that for every $j = 2, \ldots, n$, the transposition $(1, j)$ is in H. We prove this by induction on j. By hypothesis, we have $(1, 2) \in H$. For $j \in \{3, \ldots, n\}$, assuming that $(1, j-1) \in H$, we have

$$(1, j) = (1, j-1)(j-1, j)(1, j-1) \in H,$$

since $(j-1, j) \in H$ by equation (1). This completes the induction, proving our claim.
Third, we claim that *every* transposition in S_n lies in H. To prove this, for any indices $a < b$ in $\{1, \ldots, n\}$, let $j = b - a + 1 \in \{2, \ldots, n\}$. Then $\sigma^{a-1}(1) = a$, and $\sigma^{a-1}(j) = b$, and hence

$$(a, b) = \sigma^{a-1}(1, j)\sigma^{-a+1} \in H,$$

since $(1, j) \in H$ by our previous claim.
Finally, it is a standard fact in Math 350 that the transpositions generate S_n. Since H contains all the transpositions, we must have $H = S_n$. QED

[**Note 1**. For $n \geq 4$ not prime, it's important for the above fact that the n-cycle σ have the two elements of the transposition τ appear *consecutively*; otherwise, σ and τ might *not* generate all of S_n. For example, in S_4, $(1, 3)$ and $(1, 2, 3, 4)$ together generate only an 8-element subgroup isomorphic to D_4. More precisely, number the vertices of a square $1, 2, 3, 4$ clockwise. Then $(1, 2, 3, 4)$ corresponds to rotating the square 90° clockwise, and $(1, 3)$ corresponds to flipping it across the diagonal from vertex 2 to vertex 4. So together, $(1, 2, 3, 4)$ and $(1, 3)$ only generate that 8-element subgroup of S_4.]

[**Note 2**. On the other hand, if $n = p$ is prime, then *any* p-cycle σ and *any* transposition τ will together generate all of S_p. That fact can be proven as follows. First, after re-labeling the p indices being permuted, we can assume without loss that $\tau = (1, 2)$. Second, since p is prime, we can show that *some* power σ^j of σ maps 1 to 2. But again because p is prime, σ^j is still a p-cycle. Relabeling the remaining indices $3, 4, \ldots, p$ if necessary, then, we can write $\sigma^j = (1, 2, \ldots, p)$, while still preserving the fact that $\tau = (1, 2)$. Finally, apply the result of this exercise, and we're done.]