6.1#3: (a) Let \( \phi : L_1 \cong L_2 \) be an isomorphism of fields. Given a subfield \( F_1 \subseteq L_1 \), set \( F_2 = \phi(F_1) \), which is a subfield of \( L_2 \). Prove that the map sending \( \sigma \in \text{Gal}(L_1/F_1) \) to \( \phi \circ \sigma \circ \phi^{-1} \) induces an isomorphism \( \text{Gal}(L_1/F_1) \cong \text{Gal}(L_2/F_2) \). (b) Explain why Proposition 6.1.11 follows from part (a).

**Proof. (a): (Function):** Given \( \sigma \in \text{Gal}(L_1/F_1) \), we must first show that \( \phi \circ \sigma \circ \phi^{-1} \in \text{Gal}(L_2/F_2) \). To see this, first note that \( \phi^{-1} : L_2 \rightarrow L_1, \sigma : L_1 \rightarrow L_1 \), and \( \phi : L_1 \rightarrow L_2 \) are field isomorphisms, and hence their composition \( \phi \circ \sigma \circ \phi^{-1} : L_2 \rightarrow L_2 \) is also an isomorphism. In addition, for any \( b \in F_2 \), we have \( \phi^{-1}(b) \in F_1 \), and hence \( \sigma(\phi^{-1}(b)) = \phi^{-1}(b) \). Therefore, \( \phi \circ \sigma \circ \phi^{-1}(b) = \phi(\phi^{-1}(b)) = b \) for every \( b \in F_2 \). Thus, we have shown that \( \phi \circ \sigma \circ \phi^{-1} \in \text{Gal}(L_2/F_2) \), as desired.

It follows that we may define a function \( \Phi : \text{Gal}(L_1/F_1) \rightarrow \text{Gal}(L_2/F_2) \) by \( \Phi(\sigma) = \phi \circ \sigma \circ \phi^{-1} \). We must now show that \( \Phi \) is a bijective group homomorphism.

**(Homomorphism):** Given \( \sigma, \tau \in \text{Gal}(L_1/F_1) \), we have
\[
\Phi(\sigma \circ \tau) = \phi \circ \sigma \circ \tau \circ \phi^{-1} = \phi \circ \sigma \circ \phi^{-1} \circ \phi \circ \tau \circ \phi^{-1} = \Phi(\sigma) \circ \Phi(\tau).
\]

**(Bijective):** By the reasoning of the first part of this proof, we may define a function \( \Psi : \text{Gal}(L_2/F_2) \rightarrow \text{Gal}(L_1/F_1) \) by \( \Psi(\sigma) = \phi^{-1} \circ \sigma \circ \phi \). Then for any \( \sigma \in \text{Gal}(L_1/F_1) \), we have
\[
\Psi(\Phi(\sigma)) = \Psi(\phi \circ \sigma \circ \phi^{-1}) = \phi^{-1} \circ \phi \circ \sigma \circ \phi^{-1} = \phi = \sigma.
\]
Similarly, for any \( \sigma \in \text{Gal}(L_2/F_2) \), we have
\[
\Phi(\Psi(\sigma)) = \Phi(\phi^{-1} \circ \sigma \circ \phi) = \phi \circ \phi^{-1} \circ \sigma \circ \phi \circ \phi^{-1} = \sigma.
\]

Thus, \( \Phi \) is an invertible function (with inverse \( \Psi \)), as desired. \( \square \)

(b) In Proposition 6.1.11, we are given finite extensions \( L_1/F \) and \( L_2/F \) and a field isomorphism \( \phi : L_1 \rightarrow L_2 \) that is the identity on \( F \). Define \( F_1 = F \) and \( F_2 = F \). Then we are in the situation of part (a), and hence \( \text{Gal}(L_1/F) \cong \text{Gal}(L_2/F) \) via \( \sigma \mapsto \phi \circ \sigma \circ \phi^{-1} \). \( \square \)

6.1#5(b), strengthened: Prove that \( |\text{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q})| = 2^n \), where \( p_1, \ldots, p_n \) are the first \( n \) primes.

**Proof.** We will prove the following (stronger) lemma:

**Lemma.** Let \( m_1, \ldots, m_n \in \mathbb{Z} \) be pairwise relatively prime squarefree integers, none of which is \( 1 \). Then \( \sqrt{m_n} \notin \mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_{n-1}}) \).

**Proof of Lemma.** We proceed by induction on \( n \).

**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.

If \( a = 0 \), then \( \sqrt{m_{n-1}m_n} = bm_{n-1} \in K \), again contradicting the inductive hypothesis, since \( \{m_1, \ldots, m_{n-2}\} \cup \{m_{n-1} \cdot m_n\} \) forms 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 \( \sqrt{m_{n-1}} = (2ab)^{-1}(m_n - a^2 - b^2m_{n-1}) \in K \), again contradicting the inductive hypothesis. \( \square \)
For each $i = 0, \ldots, n$, let $K_i = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_i}) = K_{i-1}(\sqrt{p_i})$. By the Lemma, we have $\sqrt{p_i} \notin K_{i-1}$, and hence the quadratic polynomial $x^2 - p_i$ is irreducible over $K_{i-1}$, and therefore $[K_i : K_{i-1}] = 2$.

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 $|\text{Gal}(K_n/\mathbb{Q})| = [K_n : \mathbb{Q}] = 2^n$. \qed

6.2#5: Let $\text{char } F = p$, and suppose $f = x^p - x + a \in F[x]$ is irreducible over $F$. Let $L = F(\alpha)$, where $\alpha$ is a root of $f$; in Exercise 5.3.16, you showed $L/F$ is normal and separable. (a) Prove $|\text{Gal}(L/F)| = p$, and that $\text{Gal}(L/F) \cong \mathbb{Z}/p\mathbb{Z}$. (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 $\text{Gal}(L/F)$ that takes $\alpha$ to $\alpha + i$.

(c) Find an explicit isomorphism $\text{Gal}(L/F) \cong \mathbb{Z}/p\mathbb{Z}$.

**Proof.** (a): We claim $L$ is the splitting field of $f$ over $F$. Indeed, by the facts quoted from Exercise 5.3.16, $L/F$ is normal; since it contains one root of the irreducible polynomial $f$, it follows that $f$ splits over $L$. On the other hand, since $\alpha$ is one root of $f$, then $L = F(\alpha)$ must be contained in the splitting field, proving our claim. In addition, $f$ is separable (again from Exercise 5.3.16), so by Theorem 6.2.1, we have $|\text{Gal}(L/F)| = |L : F| = p$, where the second equality is because $\deg(f) = p$ and $f$ is irreducible over $F$. Finally, from Math 350, every group of prime order is cyclic, so $\text{Gal}(L/F) \cong \mathbb{Z}/p\mathbb{Z}$.

(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 $\text{char } F = p$.

By Proposition 5.1.8, for each $i \in \mathbb{Z}$, there is some $\sigma_i \in \text{Gal}(L/F)$ 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 $\text{Gal}(L/F)$. Therefore, for each $i = 0, 1, \ldots, p - 1$, there is one and only one map in $\text{Gal}(L/F)$ that takes $\alpha$ to $\alpha + i$, namely $\sigma_i$.

(c): Define $\phi : \mathbb{Z} \rightarrow \text{Gal}(L/F)$ by $\phi(i) = \sigma_i$. Since part (b) gives us $\text{Gal}(L/F) = \{\sigma_0, \sigma_1, \ldots, \sigma_{p-1}\}$, it is immediate that $\phi$ is surjective. To see that $\phi$ 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 $\tau \in \text{Gal}(L/F)$ 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 $\text{char } F = p$, 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 $\sigma_i = \text{id}_L$, so $i \in \ker(\phi)$, proving the claim.

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

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

\qed
6.3#3. What known group is $\text{Gal}(\mathbb{Q}(i, \sqrt{2}, \sqrt{3})/\mathbb{Q})$ isomorphic to? Explain/prove your claim.

**Proof.** Let $L = \mathbb{Q}(i, \sqrt{2}, \sqrt{3})$ and $G = \text{Gal}(L/\mathbb{Q})$. We claim $G \cong C_2 \times C_2 \times C_2$.

First, we know $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ from earlier examples. Since $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{R}$, we have $i \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and hence $[L : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2$. By the Tower Theorem, $[L : \mathbb{Q}] = 8$, and hence by Theorem 6.2.1, we have $|\text{Gal}(L/F)| = 8$. **[Note:** Alternatively, we could simply quote the strengthened $\sqrt{m_1}, \ldots, \sqrt{m_n}$ result from Exercise 6.1.3 to get $|\text{Gal}(L/F)| = 8$ instantly.]

Next, by Proposition 6.1.4(a) applied to each of $i, \sqrt{2}, \sqrt{3}$, for any $\sigma \in \text{Gal}(L/F)$, we have
\[
\sigma(i) = \pm i, \quad \sigma(\sqrt{2}) = \pm \sqrt{2}, \quad \sigma(\sqrt{3}) = \pm \sqrt{3}.
\]
Thus, writing $C_2$ as $\{\pm 1\}$ under multiplication, we may define $\phi : G \to C_2 \times C_2 \times C_2$ by
\[
\phi(\sigma) = \left( \frac{\sigma(i)}{i}, \frac{\sigma(\sqrt{2})}{\sqrt{2}}, \frac{\sigma(\sqrt{3})}{\sqrt{3}} \right).
\]
By Proposition 6.1.4(b), $\sigma$ is determined by the values $\sigma(i), \sigma(\sqrt{2}), \sigma(\sqrt{3})$, and hence $\phi$ is injective. Because $|\text{Gal}(L/F)| = 8 = |C_2 \times C_2 \times C_2|$, it follows by the pigeonhole principle that $\phi$ is also surjective. Finally, to show $\phi$ is a group homomorphism, given $\sigma, \tau \in \text{Gal}(L/F)$, we have
\[
\phi(\sigma \tau) = \left( \frac{\sigma \tau(i)}{\tau(i)}, \frac{\sigma \tau(\sqrt{2})}{\sqrt{2}}, \frac{\sigma \tau(\sqrt{3})}{\sqrt{3}} \right) = \left( \frac{\sigma(i)}{i}, \frac{\sigma(\sqrt{2})}{\sqrt{2}}, \frac{\sigma(\sqrt{3})}{\sqrt{3}} \right) \cdot \left( \frac{\tau(i)}{\tau(i)}, \frac{\tau(\sqrt{2})}{\sqrt{2}}, \frac{\tau(\sqrt{3})}{\sqrt{3}} \right) = \phi(\sigma) \cdot \phi(\tau),
\]
where the fourth equality is because each of $\tau(i)/i, \tau(\sqrt{2})/\sqrt{2}, \tau(\sqrt{3})/\sqrt{3}$ lies in $\{\pm 1\} \subseteq \mathbb{Q}$. 

**Note:** An alternative strategy, after proving that $|\text{Gal}(L/F)| = 8$, and observing that any $\sigma \in \text{Gal}(L/F)$ is determined by $\sigma(i), \sigma(\sqrt{2}), \sigma(\sqrt{3})$ as above, would be to prove that any such $\sigma$ satisfies $\sigma^2 = e$. Thus, $G$ is a group of order 8 such that every non-identity element has order 2. Then results from Math 350 show that $G$ must be isomorphic to $C_2 \times C_2 \times C_2$.

6.3#4. Let $\alpha = \sqrt{2} + \sqrt{3}$, and let $L = \mathbb{Q}(\alpha)$. In Exercise 5.1.6, you showed that $f = x^4 - 4x^2 - 2$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}$, with splitting field $L$. Prove that $\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

**Proof.** Since $L = \mathbb{Q}(\alpha)$ and $f$ is irreducible over $\mathbb{Q}$, we have $|\text{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = \deg f = 4$. We saw in Exercise 5.1.6 that the four roots of $f$ are $\pm \alpha$ and $\pm \beta$, where $\beta = \sqrt{2} - \sqrt{3}$. We also saw that $\beta = (\alpha^2 - 2)/\alpha$, and that $\alpha \beta = \sqrt{2}$.

By Theorem 6.1.4, there exists $\sigma \in \text{Gal}(L/\mathbb{Q})$ such that $\sigma(\alpha) = \beta$. Therefore,
\[
\sigma(\beta) = \sigma\left( \frac{\alpha^2 - 2}{\alpha} \right) = \frac{\beta^2 - 2}{\beta} = \frac{2 - \sqrt{2} - 2}{\sqrt{2}} = -\frac{\sqrt{2}}{\sqrt{2}} = -\alpha,
\]
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 $\sigma$, denoted $o(\sigma)$, is neither 1 nor 2.

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

\[\square\]
6.3#5. Let \( g_1, \ldots, g_s \in F[x] \) with \( \deg(g_i) = d_i > 0 \), and suppose \( f = g_1 \cdots g_s \) is separable, with splitting field \( L \) over \( F \). Prove that \( \text{Gal}(L/F) \) is isomorphic to a subgroup of \( S_{d_1} \times \cdots \times S_{d_s} \).

**Proof.** For each \( i = 1, \ldots, s \), call the roots of \( g_i \) \( \alpha_{i,j} \), for \( j = 1, \ldots, d_i \). Since \( f \) is separable, we have \( \alpha_{i,j} = \alpha_{k,\ell} \) if and only if \( i = k \) and \( j = \ell \). In addition, by Proposition 6.1.4, for each \( i = 1, \ldots, s \) and each \( \sigma \in \text{Gal}(L/F) \), we have that \( \sigma \) permutes the roots \( \{\alpha_{i,j} : j = 1, \ldots, d_i\} \). Thus, for each such \( i \) and \( \sigma \), we may define a permutation \( \tilde{\sigma}_i \in S_{d_i} \) as follows:

for each \( j \in \{1, \ldots, d_i\} \), \( \tilde{\sigma}_i(j) \) is the unique \( \ell \in \{1, \ldots, d_i\} \) such that \( \sigma(\alpha_{i,j}) = \alpha_{i,\ell} \).

Define a function \( \Phi : \text{Gal}(L/F) \to S_{d_1} \times \cdots \times S_{d_s} \) by \( \Phi(\sigma) = (\tilde{\sigma}_1, \ldots, \tilde{\sigma}_s) \). We claim that \( \Phi \) is an injective group homomorphism.

To see this, given \( \sigma, \tau \in \text{Gal}(L/F) \), observe that for any \( i, j, k, \ell \), if \( \tau(\alpha_{i,j}) = \alpha_{i,k} \) and \( \sigma(\alpha_{i,k}) = \alpha_{i,\ell} \), then \( \sigma\tau(\alpha_{i,j}) = \sigma(\alpha_{i,k}) = \alpha_{i,\ell} \), and hence \( \tilde{\sigma}_i(\tau(\alpha_{i,j})) = \tilde{\sigma}_i(\alpha_{i,k}) = \tilde{\sigma}_i(\alpha_{i,\ell}) \). Thus, \( \Phi(\sigma\tau) = (\tilde{\sigma}_1 \tilde{\tau}_1, \ldots, \tilde{\sigma}_s \tilde{\tau}_s) = (\tilde{\sigma}_1 \tilde{\tau}_1, \ldots, \tilde{\sigma}_s \tilde{\tau}_s) = \Phi(\sigma)\Phi(\tau) \), as desired. Finally, by Proposition 6.1.4 again, \( \sigma \in \text{Gal}(L/F) \) is completely determined by the values of \( \sigma(\alpha_{i,j}) \), and hence by \( \Phi(\sigma) \).

Hence, \( \Phi \) is an injective homomorphism, as claimed. Let \( H \) be the image \( H = \Phi(\text{Gal}(L/F)) \), which is a subgroup of \( S_{d_1} \times \cdots \times S_{d_s} \). Then \( \Phi \) is an isomorphism from \( \text{Gal}(L/F) \) to \( H \). \( \square \)

6.4#7. Prove that \( S_n \) is generated by \((1,2)\) and \((1,2,\ldots,n)\).

**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,

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

(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 \( H = S_n \). \( \square \)

[Note 1. For \( n \geq 4 \) not prime, it’s important for the above fact that the \( n \)-cycle \( \sigma \) have the two elements of the transposition \( \tau \) appear consecutively; otherwise, \( \sigma \) and \( \tau \) 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 \(90^\circ \) 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 an 8-element subgroup of \( S_4 \).]

[Note 2. On the other hand, if \( n = p \) is prime, then any \( p \)-cycle \( \sigma \) and any transposition \( \tau \) 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 $\sigma^j$ of $\sigma$ maps 1 to 2. But again because $p$ is prime, $\sigma^j$ is still a $p$-cycle. Relabeling the remaining indices 3, 4, ..., $p$ if necessary, then, we can write $\sigma^j = (1, 2, ..., p)$, while still preserving the fact that $\tau = (1, 2)$. Finally, apply the result of this exercise, and we’re done.]

**7.1#8.** Let $h$ be the polynomial (7.1) used in the proof of Theorem 7.1.1, (b) $\Rightarrow$ (c). Prove there is an integer $m$ such that $\prod_{\sigma \in \text{Gal}(L/F)} (x - \sigma(a)) = h^m$.

**Proof.** Let $G = \text{Gal}(L/F)$. [Recall $L/F$ is a finite extension with $F = L_G$, and that $h = \prod_{i=1}^{r}(x - \alpha_i)$, where $\alpha = \alpha_1, ..., \alpha_r$ are the distinct elements of $L$ of the form $\sigma(\alpha)$, for $\sigma \in G$.] Define

$$H = \{ \sigma \in G : \sigma(\alpha) = \alpha \}.$$ 

We claim $H$ is a subgroup of $G$. It is nonempty because $e \in H$, where $e = \text{id}_L$ is the identity element of $G$. Given $\sigma, \tau \in H$, we have $\sigma \tau(\alpha) = \sigma(\tau(\alpha)) = \alpha$ and $\sigma^{-1}(\alpha) = \alpha$, so $H$ is closed under composition and inverses, proving our claim. Let $m = |H|$.

For each $i = 1, ..., r$, by definition of $\alpha_i$, there exists $\tau_i \in G$ such that $\alpha_i = \tau_i(\alpha)$. Then the left coset $\tau_iH$ also has cardinality $|\tau_iH| = m$, by Math 350. We make a second claim, that $\tau_iH = J_i$, where

$$J_i = \{ \sigma \in G : \sigma(\alpha) = \alpha_i \}.$$ 

To prove $\tau_iH \subseteq J_i$, any $\sigma \in \tau_iH$ is of the form $\tau_i \eta$ for some $\eta \in H$, whence $\sigma(\alpha) = \tau_i(\eta(\alpha)) = \tau_i(\alpha) = \alpha_i$, so $\sigma \in J_i$. Conversely, given $\sigma \in J_i$, define $\eta = \tau_i^{-1}(\sigma(\alpha)) = \tau_i^{-1}(\alpha_i) = \alpha$, so that $\eta \in H$, and hence $\sigma = \tau_i \eta \in \tau_iH$, proving our second claim.

On the other hand, $J_i \cap J_j = \emptyset$ for $i \neq j$, since $\alpha_i \neq \alpha_j$. Thus, $G$ is a disjoint union $G = J_1 \cup \cdots \cup J_r$, and so

$$\prod_{\sigma \in \text{Gal}(L/F)} (x - \sigma(a)) = \prod_{i=1}^{r} \left[ \prod_{\sigma \in J_i} (x - \sigma(\alpha)) \right] = \prod_{i=1}^{r} \left[ \prod_{\sigma \in J_i} (x - \alpha_i) \right] = \prod_{i=1}^{r} (x - \alpha_i)^m = h^m,$$

as desired.

**7.1#9.** Decide whether each of the following extensions is Galois, and justify [probably using Theorems 7.1.1 and 1.5(c)]:

(a) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q}$. (b) $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$, where $\alpha, \beta$ are distinct roots of $x^3 + x^2 + 2x + 1$. (c) $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$.

(d) $\mathbb{C}(t)/\mathbb{C}(t + t^{-1})$. (e) $\mathbb{C}(t)/\mathbb{C}(t^n)$.

**Answers/Proofs.** (a): Not Galois. Observe that $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ has $L \subseteq \mathbb{R}$. However, the irreducible polynomial $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ has one root in $L$ (namely $\sqrt[3]{2}$). We know that $\beta = \zeta_3 \sqrt[3]{2}$ is another root of $f$, and that $\beta \not\in \mathbb{R}$, so $\beta \not\in L$. Thus, $f$ has a root in $L$ but does not split completely in $L$, so $L/\mathbb{Q}$ is not a normal extension, and hence not Galois. (That’s condition (c) of Theorem 7.1.1.)

(b): Galois. Let $L = \mathbb{Q}(\alpha, \beta)$, and let $\gamma$ be the third root of $f(x) = x^3 + x^2 + 2x + 1$ Since the $x^2$-coefficient of $f$ is 1, we have $\alpha + \beta + \gamma = -1$, and hence $\gamma = -1 - \alpha - \beta \in L$. Thus, $f$ splits completely over $L$.

We claim that $f$ is separable. There are various ways to see this. One would be to run the Euclidean algorithm on $f$ and $f' = 3x^2 + 2x + 2$ to verify that $\gcd(f, f') = 1$, and invoke Proposition 5.3.2. A less computational way is to observe that $f$ is irreducible: if $f$ is reducible over $\mathbb{Q}$, then being a cubic polynomial, it has a root $a \in \mathbb{Q}$. Writing $a = m/n$ in lowest terms, we have $n = 1$ (and hence $a = m$) because $f \in \mathbb{Z}[x]$ is monic, and hence looking at the constant term, we have $m|1$, so that
To prove (c): Note Galois. Let $F = \mathbb{F}_p(t^p)$ and $L = \mathbb{F}_p(t)$. Then $t \in L$ is a root of $f(x) = x^p - t^p$, which is an irreducible polynomial in $F[x]$, by Proposition 4.2.6. That is, $t \in L$ has minimal polynomial $f$ over $F$, but $f(x) = (x - t)^p$ is not separable. Thus, by definition, $t$ is not separable over $F$. Also by definition, then, $L/F$ is not a separable extension, and hence not Galois. (That’s condition (c) of Theorem 7.1.1.)

(d): Galois. Let $F = \mathbb{C}(t + t^{-1})$ and $L = \mathbb{C}(t)$. Let $u = t + t^{-1}$. Motivated by the computation $tu = t^2 + 1$, we see that $t \in L$ is a root of $f(x) = x^2 - ux + 1 \in F[x]$. The two roots of $f$ are $t, t^{-1} \in L$, which are distinct, so $f$ is separable. Moreover, $L = F(t) = F(t, t^{-1})$ is the splitting field of $f$ over $F$. Thus, $L$ is the splitting field of the separable polynomial $f$ over $F$, so by Theorem 7.1.1(a), it is Galois over $F$.

(e): Galois. Let $F = \mathbb{C}(t^n)$, let $L = \mathbb{C}(t)$, and let $f(x) = x^n - t^n \in F[x]$. Then the $n$ roots of $f$ are $\{\zeta^n_0 t : j = 0, 1, \ldots, n - 1\} \subseteq L$, which are all distinct, so $f$ is separable. In addition, because $\zeta_n \in \mathbb{C} \subseteq F$, we have $L = F(t) = F(t, \zeta_n t, \ldots, \zeta_n^{n-1} t)$, and hence $L$ is the splitting field of $f$ over $F$. Thus, $L$ is the splitting field of the separable polynomial $f$ over $F$, so by Theorem 7.1.1(a), it is Galois over $F$.

7.2#1. In diagram (7.3) [of the subextensions of $Q(\omega, \sqrt[3]{2})$], prove: (a) $Q(\sqrt[3]{2})$ has conjugate fields $Q(\sqrt{2})$, $Q(\omega \sqrt[3]{2})$, and $Q(\omega^2 \sqrt{2})$. (b) $Q(\omega)$ equals all of its conjugates.

Proof. Let $\alpha = \sqrt[3]{2}$, let $L = Q(\omega, \alpha)$, and let $G = \text{Gal}(L/Q)$.

(a): From past examples, we know that for all $\sigma \in G$, we have $\sigma(\alpha) = \omega^j \alpha$ for some $j = 0, 1, 2$; we also know that each of $j = 0, 1, 2$ is attained by some $\sigma \in G$.

For each $j = 0, 1, 2$, let $K_j = Q(\omega^j \alpha)$; we must show that $K_j$ is a conjugate of $K_0$. To do so, pick $\sigma \in G$ such that $\sigma(\alpha) = \omega^j \alpha$; we will prove that $K_j = \sigma K_0$.

To prove $\supseteq$: Given $\gamma \in \sigma K_0$, we have $\gamma = \sigma(\beta)$ for some $\beta \in K_0$. Then by definition, $\beta = h(\alpha)$ for some rational function $h(x) \in Q(x)$. Hence,

$$\gamma = \sigma(h(\alpha)) = h(\sigma(\alpha)) = h(\omega^j \alpha) \in K_j.$$ 

To prove $\subseteq$: Given $\gamma \in K_j$, we may write $\gamma = h(\omega^j \alpha)$ for some rational function $h(x) \in Q(x)$. Hence,

$$\gamma = h(\omega^j \alpha) = h(\sigma(\alpha)) = h(\sigma(h(\alpha))) \in \sigma K_0.$$ 

(b): Let $M = Q(\omega)$. Given $\sigma \in G$, we know from past examples that $\sigma(\omega) = \omega^j$ for some $j = 1, 2$. For each choice of $j$, we must show that $\sigma M = M$.

To prove $\subseteq$: Given $\gamma \in \sigma M$, we have $\gamma = \sigma(\beta)$ for some $\beta \in M$. Then by definition, $\beta = h(\omega)$ for some rational function $h(x) \in Q(x)$. Hence,

$$\gamma = \sigma(h(\omega)) = h(\sigma(\omega)) = h(\omega^j) \in M.$$ 

To prove $\supseteq$: Given $\gamma \in M$, we may write $\gamma = h(\omega)$ for some rational function $h(x) \in Q(x)$. Observe that $\sigma(\omega^j) = (\omega^j)^j = \omega$ for both $j = 1$ and $j = 2$. Thus,

$$\gamma = h(\omega) = h(\sigma(\omega^j)) = \sigma(h(\omega^j)) \in \sigma M.$$ 

□