12. We should note that $\overline{\mathbb{Q}(x)}$ is an algebraic closure of $\overline{\mathbb{Q}}(x)$. We know that π is transcendental over $\mathbb{Q}$. Therefore, $\sqrt{\pi}$ must be transcendental over $\mathbb{Q}$, for if it were algebraic, then $\pi = (\sqrt{\pi}\,)^2$ would be algebraic over $\mathbb{Q}$, because algebraic numbers form a closed set under field operations. Therefore the map $\tau : \mathbb{Q}(\sqrt{\pi}\,) \to \mathbb{Q}(x)$ where $\tau(a) = a$ for $a \in \mathbb{Q}$ and $\tau(\sqrt{\pi}\,) = x$ is an isomorphism. Theorem 49.3 shows that τ can be extended to an isomorphism σ mapping $\overline{\mathbb{Q}(\sqrt{\pi}\,)}$ onto a subfield of $\overline{\mathbb{Q}(x)}$. Then σ^{-1} is an isomorphism mapping $\sigma[\overline{\mathbb{Q}(\sqrt{\pi}\,)}]$ onto a subfield of $\overline{\mathbb{Q}(\sqrt{\pi}\,)}$ which can be extended to an isomorphism of $\overline{\mathbb{Q}(x)}$ onto a subfield of $\overline{\mathbb{Q}(\sqrt{\pi}\,)}$. But because σ^{-1} is already onto $\overline{\mathbb{Q}(\sqrt{\pi}\,)}$, we see that σ must actually be onto $\overline{\mathbb{Q}(x)}$, so σ provides the required isomorphism of $\overline{\mathbb{Q}(\sqrt{\pi}\,)}$ with $\overline{\mathbb{Q}(x)}$.

13. Let E be a finite extension of F. Then by Theorem 31.11, $E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ where each α_i is algebraic over F. Now suppose that $L = F(\alpha_1, \alpha_2, \cdots, \alpha_{k+1})$ and $K = F(\alpha_1, \alpha_2, \cdots, \alpha_k)$. Every isomorphism of L onto a subfield of $\overline{F}$ and leaving F fixed can be viewed as an extension of an isomorphism of K onto a subfield of $\overline{F}$. The extension of such an isomorphism τ of K to an isomorphism σ of L onto a subfield of $\overline{F}$ is completely determined by $\sigma(\alpha_{k+1})$. Let $p(x)$ be the irreducible polynomial for α_{k+1} over K, and let $q(x)$ be the polynomial in $\tau[K][x]$ obtained by applying τ to each of the coefficients of $p(x)$. Because $p(\alpha_{k+1}) = 0$, we must have $q(\sigma(\alpha_{k+1})) = 0$, so the number of choices for $\sigma(\alpha_{k+1})$ is at most $\deg(q(x)) = \deg(p(x)) = [L : K]$. Thus $\{L : K\} \leq [L : K]$, that is

$$\{F(\alpha_1, \cdots, \alpha_{k+1}) : F(\alpha_1, \cdots, \alpha_k)\} \leq [F(\alpha_1, \cdots, \alpha_{k+1}) : F(\alpha_1, \cdots, \alpha_k)]. \tag{1}$$

We have such an inequality (1) for each $k = 1, 2, \cdots, n-1$. Using the multiplicative properties of the index and of the degree (Corollaries 49.10 and 31.6), we obtain upon multiplication of these $n-1$ inequalities the desired result, $\{E : F\} \leq [E : F]$.

50. Splitting Fields

1. The splitting field is $\mathbb{Q}(\sqrt{3})$ and the degree over $\mathbb{Q}$ is 2.

2. Now $x^4 - 1 = (x-1)(x+1)(x^2+1)$. The splitting field is $\mathbb{Q}(i)$ and the degree over $\mathbb{Q}$ is 2.

3. The splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and the degree over $\mathbb{Q}$ is 4.

4. The splitting field has degree 6 over $\mathbb{Q}$. Replace $\sqrt[3]{2}$ by $\sqrt[3]{3}$ in Example 50.9.

5. Now $x^3 - 1 = (x-1)(x^2+x+1)$. The splitting field has degree 2 over $\mathbb{Q}$.

6. The splitting field has degree $2 \cdot 6 = 12$ over $\mathbb{Q}$. See Example 50.9 for the splitting field of $x^3 - 2$.

7. We have $|G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}| = 1$, because $\sqrt[3]{2} \in \mathbb{R}$ and the other conjugates of $\sqrt[3]{2}$ do not lie in $\mathbb{R}$ (see Example 50.9). They yield isomorphisms into $\mathbb{C}$ rather than automorphisms of $\mathbb{Q}(\sqrt[3]{2})$.

8. We have $|G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}| = 6$, because $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ is the splitting field of $x^3 - 2$ and is of degree 6, as shown in Example 50.9.

9. $|G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(\sqrt[3]{2})| = 2$, because $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ is the splitting field of $x^2 + 3$ over $\mathbb{Q}(\sqrt[3]{2})$.

10. Theorem 33.3 shows that the only field of order 8 in $\overline{\mathbb{Z}_2}$ is the splitting field of $x^8 - x$ over $\mathbb{Z}_2$. Because a field of order 8 can be obtained by adjoining to $\mathbb{Z}_2$ a root of any cubic polynomial that is irreducible in $\mathbb{Z}_2[x]$, it must be that all roots of every irreducible cubic lie in this unique subfield of order 8 in $\overline{\mathbb{Z}_2}$.

11. The definition is incorrect. Insert "irreducible" before "polynomial".

Let $F \leq E \leq \overline{F}$ where $\overline{F}$ is an algebraic closure of a field F. The field E is a **splitting field over** F if and only if E contains all the zeros in $\overline{F}$ of every irreducible polynomial in $F[x]$ that has a zero in E.

12. The definition is incorrect. Replace "lower degree" by "degree one".

A polynomial $f(x)$ in $F[x]$ **splits in an extension field** E of F if and only if it factors in $E[x]$ into a product of polynomials of degree one.

13. We have $1 \leq [E : F] \leq n!$. The example $E = F = \mathbb{Q}$ and $f(x) = x^2 - 1$ shows that the lower bound 1 cannot be improved unless we are told that $f(x)$ is irreducible over F. Example 50.9 shows that the upper bound $n!$ cannot be improved.

14. T F T T T F F T T

15. Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{2})$. Then $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ has a zero in E, but does not split in E.

16. **a.** This multiplicative relation is not necessarily true. Example 50.9 and Exercise 7 show that $6 = |G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q})| \neq |G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(\sqrt[3]{2}))| \cdot |G(\mathbb{Q}\sqrt[3]{2})/\mathbb{Q})| = 2 \cdot 1 = 2$.

b. Yes, because each field is a splitting field of the one immediately under it. If E is a splitting field over F then $|G(E/F)| = \{E : F\}$, and the index is multiplicative by Corollary 49.10.

17. Let E be the splitting field of a set S of polynomials in $F[x]$. If $E = F$, then E is the splitting field of x over F. If $E \neq F$, then find a polynomial $f_1(x)$ in S that does not split in F, and form its splitting field, which is a subfield E_1 of E where $[E_1 : F] > 1$. If $E = E_1$, then E is the splitting field of $f_1(x)$ over F. If $E \neq E_1$, find a polynomial $f_2(x)$ in S that does not split in E_1, and form its splitting field $E_2 \leq E$ where $[E_2 : E_1] > 1$. If $E = E_2$, then E is the splitting field of $f_1(x)f_2(x)$ over F. If $E \neq E_2$, then continue the construction in the obvious way. Because by hypothesis E is a *finite* extension of F, this process must eventually terminate with some $E_r = E$, which is then the splitting field of the product $g(x) = f_1(x)f_2(x) \cdots f_r(x)$ over F.

18. Find $\alpha \in E$ that is not in F. Now α is algebraic over F, and must be of degree 2 because $[E : F] = 2$ and $[F(\alpha) : F] = \deg(\alpha, F)$. Thus $\text{irr}(\alpha, F) = x^2 + bx + c$ for some $b, c \in F$. Because $\alpha \in E$, this polynomial factors in $E[x]$ into a product $(x - \alpha)(x - \beta)$, so the other root β of $\text{irr}(\alpha, F)$ lies in E also. Thus E is the splitting field of $\text{irr}(\alpha, F)$.

19. Let E be a splitting field over F. Let α be in E but not in F. By Corollary 50.6, the polynomial $\text{irr}(\alpha, F)$ splits in E since it has a zero α in E. Thus E contains all conjugates of α over F.

Conversely, suppose that E contains all conjugates of $\alpha \in E$ over F, where $F \leq E \leq \overline{F}$. Because an automorphism σ of $\overline{F}$ leaving F fixed carries every element of $\overline{F}$ into one of its conjugates over F, we see that $\sigma(\alpha) \in E$. Thus σ induces a one-to-one map of E into E. Because the same is true of σ^{-1}, we see that σ maps E onto E, and thus induces an automorphism of E leaving F fixed. Theorem 50.3 shows that under these conditions, E is a splitting field of F.

20. Because $\mathbb{Q}(\sqrt[3]{2})$ lies in $\mathbb{R}$ and the other two conjugates of $\sqrt[3]{2}$ do not lie in $\mathbb{R}$, we see that no map of $\sqrt[3]{2}$ into any conjugate other than $\sqrt[3]{2}$ itself can give rise to an automorphism of $\mathbb{Q}(\sqrt[3]{2})$; the other two maps give rise to isomorphisms of $\mathbb{Q}(\sqrt[3]{2})$ onto a subfield of $\overline{\mathbb{Q}}$. Because any automorphism of $\mathbb{Q}(\sqrt[3]{2})$ must leave the prime field $\mathbb{Q}$ fixed, we see that the identity is the only automorphism of $\mathbb{Q}(\sqrt[3]{2})$. [For an alternate argument, see Exercise 39 of Section 48.]

21. The conjugates of $\sqrt[3]{2}$ over $\mathbb{Q}(i\sqrt{3})$ are

$$\sqrt[3]{2}, \quad \sqrt[3]{2}\frac{-1+i\sqrt{3}}{2}, \quad \text{and} \quad \sqrt[3]{2}\frac{-1-i\sqrt{3}}{2}.$$

Maps of $\sqrt[3]{2}$ into each of them give rise to the only three automorphisms in $G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(i\sqrt{3}))$. Let σ be the automorphism such that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\frac{-1+i\sqrt{3}}{2}$. Then σ must be a generator of this group of order 3, because σ is not the identity map, and every group of order 3 is cyclic. Thus the automorphism group is isomorphic to $\mathbb{Z}_3$.

22. **a.** Each automorphism of E leaving F fixed is a one-to-one map that carries each zero of $f(x)$ into one of its conjugates, which must be a zero of an irreducible factor of $f(x)$ and hence is also a zero of $f(x)$. Thus each automorphism gives rise to a one-to-one map of the set of zeros of $f(x)$ onto itself, that is, it acts as a permutation on the zeros of $f(x)$.

b. Because E is the splitting field of $f(x)$ over F, we know that $E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ where $\alpha_1, \alpha_2, \cdots, \alpha_n$ are the zeros of $f(x)$. As Exercise 33 of Section 48 shows, an automorphism σ of E leaving F fixed is completely determined by the values $\sigma(\alpha_1), \sigma(\alpha_2), \cdots, \sigma(\alpha_n)$ that is, by the permutation of the zeros of $f(x)$ given by σ.

c. We associate with each $\sigma \in G(E/F)$ its permutation of the zeros of $f(x)$ in E. Part(**b**) shows that different elements of $G(E/F)$ produce different permutations of the zeros of $f(x)$. Because multiplication $\sigma\tau$ in $G(E/F)$ is function composition and because multiplication of the permutations of zeros is again composition of these same functions, with domain restricted to the zeros of $f(x)$, we see that $G(E/F)$ is isomorphic to a subgroup of the group of all permutations of the zeros of $f(x)$.

23. **a.** We have $|\,G(E/\mathbb{Q})| = 2 \cdot 3 = 6$, because $\{\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}\} = 2$ since $\text{irr}(i\sqrt{3}, \mathbb{Q}) = x^2 + 3$ and $\{\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(i\sqrt{3})\} = 3$ because $\text{irr}(\sqrt[3]{2}, \mathbb{Q}(i\sqrt{3})) = x^3 - 2$. The index is multiplicative by Corollary 49.10.

b. Because E is the splitting field of $x^3 - 2$ over $\mathbb{Q}$, Exercise 22 shows that $G(E/\mathbb{Q})$ is isomorphic to a subgroup of the group of all permutations of the three zeros of $x^3 - 2$ in E. Because the group of all permutations of three objects has order 6 and $|G(E/\mathbb{Q})| = 6$ by Part(**a**), we see that $G(E/\mathbb{Q})$ is isomorphic to the full symmetric group on three letters, that is, to S_3.

24. We have $x^p = (x-1)(x^{p-1}+\cdots+x+1)$, and Corollary 23.17 shows that the second of these factors, the cyclotomic polynomial $\Phi_p(x)$, is irreducible over the field $\mathbb{Q}$. Let ζ be a zero of $\Phi_p(x)$ in its splitting field over $\mathbb{Q}$. Exercise 36a of Section 48 shows that then $\zeta, \zeta^2, \zeta^3, \cdots, \zeta^{p-1}$ are distinct and are all zeros of $\Phi_p(x)$. Thus all zeros of $\Phi_p(x)$ lie in the simple extension $\mathbb{Q}(\zeta)$, so $\mathbb{Q}(\zeta)$ is the splitting field of $x^p - 1$ and of course has degree $p - 1$ over $\mathbb{Q}$ because $\Phi_p(x) = \text{irr}(\zeta, \mathbb{Q})$ has degree $p - 1$.

25. By Corollary 49.5, there exists an isomorphism $\phi : \overline{F} \to \overline{F'}$ leaving each element of F fixed. Because the coefficients of $f(x) \in F[x]$ are all left fixed by ϕ, we see that ϕ carries each zero of $f(x)$ in $\overline{F}$ into a zero of $f(x)$ in $\overline{F'}$. Because the zeros of $f(x)$ in $\overline{F}$ generate its splitting field E in $\overline{F}$, we see that $\phi[E]$ is contained in the splitting field E' of $f(x)$ in $\overline{F'}$. But the same argument can be made for ϕ^{-1}; we must have $\phi^{-1}[E'] \subseteq E$. Thus ϕ maps E onto E', so these two splitting fields of $f(x)$ are isomorphic.

51. Separable Extensions

1. Because $\sqrt[3]{2}\sqrt{2} = 2^{1/3}2^{1/2} = 2^{5/6}$, we have $\sqrt[6]{2} = 2/(\sqrt[3]{2}\sqrt{2})$ so $\mathbb{Q}(\sqrt[6]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$. Because $\sqrt[3]{2} = (\sqrt[6]{2})^2$ and $\sqrt{2} = (\sqrt[6]{2})^3$, we have $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}) \subseteq \mathbb{Q}(\sqrt[6]{2})$, so $\mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$. We can take $\alpha = \sqrt[6]{2}$.

2. Because $(\sqrt[4]{2})^3(\sqrt[6]{2}) = 2^{3/4}2^{1/6} = 2^{9/12}2^{2/12} = 2^{11/12}$, we see that $\sqrt[12]{2} = 2/[(\sqrt[4]{2})^3(\sqrt[6]{2})]$ so $\mathbb{Q}(\sqrt[12]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$. Because $\sqrt[4]{2} = (\sqrt[12]{2})^3$ and $\sqrt[6]{2} = (\sqrt[12]{2})^2$, we have $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2}) \subseteq \mathbb{Q}(\sqrt[12]{2})$, so $\mathbb{Q}(\sqrt[12]{2}) = \mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$. We can take $\alpha = \sqrt[12]{2}$.

3. We try $\alpha = \sqrt{2} + \sqrt{3}$. Squaring and cubing, we find that $\alpha^2 = 5 + 2\sqrt{2}\sqrt{3}$ and $\alpha^3 = 11\sqrt{2} + 9\sqrt{3}$. Because

$$\sqrt{2} = \frac{\alpha^3 - 9\alpha}{2} \text{ and } \sqrt{3} = \frac{11\alpha - \alpha^3}{2},$$

we see that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

4. Of course $\mathbb{Q}(i\sqrt[3]{2}) \subseteq \mathbb{Q}(i, \sqrt[3]{2})$. Because $i = -(i\sqrt[3]{2})^3/2$ and $\sqrt[3]{2} = -2/(i\sqrt[3]{2})^2$, we see that $\mathbb{Q}(i, \sqrt[3]{2}) \subseteq \mathbb{Q}(i\sqrt[3]{2})$. Thus $\mathbb{Q}(i, \sqrt[3]{2}) = \mathbb{Q}(i\sqrt[3]{2})$, so we can take $\alpha = i\sqrt[3]{2}$.

5. The definition is incorrect. Replace $F[x]$ by $\overline{F}[x]$ at the end.

Let $\overline{F}$ be an algebraic closure of a field F. The **multiplicity of a zero** $\alpha \in \overline{F}$ of a polynomial $f(x) \in F[x]$ is $\nu \in \mathbb{Z}^+$ if and only if $(x - \alpha)^\nu$ is the highest power of $x - \alpha$ that is a factor of $f(x)$ in $\overline{F}[x]$.

6. The definition is correct.

7. (See the answer in the text.)

8. F T T F F T T T T T

9. We are given that α is separable over F, so by definition, $F(\alpha)$ is a separable extension over F. Because β is separable over F, it follows that β is separable over $F(\alpha)$ because $q(x) =\text{irr}(\beta, F(\alpha))$ divides $\text{irr}(\beta, F)$ so β is a zero of $q(x)$ of multiplicity 1. Therefore $F(\alpha, \beta)$ is a separable extension of F by Theorem 51.9. Corollary 51.10 then asserts that each element of $F(\alpha, \beta)$ is separable over F. In particular, $\alpha \pm \beta, \alpha\beta$, and α/β if $\beta \neq 0$ are all separable over F.

10. We know that $[\mathbb{Z}_p(y) : \mathbb{Z}_p(y^p)]$ is at most p. If we can show that $\{1, y, y^2, \cdots, y^{p-1}\}$ is an independent set over $\mathbb{Z}_p(y^p)$, then by Theorem 30.19, this set could be enlarged to a basis for $\mathbb{Z}_p(y)$ over $\mathbb{Z}_p(y^p)$. But because a basis can have at most p elements, it would already be a basis, and $[\mathbb{Z}_p(y) : \mathbb{Z}_p(y^p)] = p$, showing that $\text{irr}(y, \mathbb{Z}_p(y^p))$ would have degree p and must therefore be $x^p - y^p$. Thus our problem is reduced to showing that $S = \{1, y, y^2, \cdots, y^{p-1}\}$ is an independent set over $\mathbb{Z}_p(y^p)$.

Suppose that

$$\frac{r_0(y^p)}{s_0(y^p)} \cdot 1 + \frac{r_1(y^p)}{s_1(y^p)} \cdot y + \frac{r_2(y^p)}{s_2(y^p)} \cdot y^2 + \cdots + \frac{r_{p-1}(y^p)}{s_{p-1}(y^p)} \cdot y^{p-1} = 0$$

where $r_i(y^p), s_i(y^p) \in \mathbb{Z}_p[y^p]$ for $i = 0, 1, 2, \cdots, p-1$. We want to show that all these coefficients in $\mathbb{Z}_p(y^p)$ must be zero. Clearing denominators, we see that it is no loss of generality to assume that all $s_i(y^p) = 1$ for $i = 0, 1, 2, \cdots, p-1$. Now the powers of y appearing in $r_i(y^p)(y^i)$ are all congruent to i modulo p, and consequently no terms in this expression can be combined with any terms of $r_j(y^p)(y^j)$ for $j \neq i$. Because y is an indeterminant, we then see that this linear combination of elements in S can be zero only if all the coefficients $r_i(y^p)$ are zero, so S is an independent set over $\mathbb{Z}_p(y^p)$, and we are done.

11. Let E be an algebraic extension of a perfect field F and let K be a finite extension of E. To show that E is perfect, we must show that K is a separable extension of E. Let α be an element of K. Because $[K : E]$ is finite, α is algebraic over E. Because E is algebraic over F, then α is algebraic over F by

Exercise 31 of Section 31. Because F is perfect, α is a zero of $\mathrm{irr}(\alpha, F)$ of multiplicity 1. Because $\mathrm{irr}(\alpha, E)$ divides $\mathrm{irr}(\alpha, F)$, we see that α is a zero of $\mathrm{irr}(\alpha, E)$ of multiplicity 1, so α is separable over E by the italicized remark preceding Theorem 51.9. Thus each $\alpha \in K$ is separable over E, so K is separable over E by Corollary 51.10.

12. Because K is algebraic over E and E is algebraic over F, we have K algebraic over F by Exercise 31 of Section 31. Let $\beta \in K$ and let $\beta_0, \beta_1, \cdots, , \beta_n$ be the coefficients in E of $\mathrm{irr}(\beta, E)$. Because β is a zero of $\mathrm{irr}(\beta, E)$ of algebraic multiplicity 1, we see that $F(\beta_0, \beta_1, \cdots, \beta_n, \beta)$ is a separable extension of $F(\beta_0, \beta_1, \cdots, \beta_n)$, which in turn is a separable extension of F by Corollary 51.10. Thus we are back to a tower of finite extensions, and deduce from Theorem 51.9 that $F(\beta_0, \beta_1, \cdots, \beta_n, \beta)$ is a separable extension of F. In particular, β is separable over F. This shows that every element of K is separable over F, so by definition, K is separable over F.

13. Exercise 9 shows that the set S of all elements in E that are separable over F is closed under addition, multiplication, and division by nonzero elements. Of course 0 and 1 are separable over F, so Exercise 9 further shows that S contains additive inverses and reciprocals of nonzero elements. Therefore S is a subfield of E.

14. a. We know that the nonzero elements of E form a cyclic group E^* of order $p^n - 1$ under multiplication, so all elements of E are zeros of $x^{p^n} - x$. (See Section 33.) Thus for $\alpha \in E$, we have

$$\begin{aligned}
{\sigma_p}^n(\alpha) &= {\sigma_p}^{n-1}(\sigma_p(\alpha)) = {\sigma_p}^{n-1}(\alpha^p) = {\sigma_p}^{n-2}(\sigma_p(\alpha^p)) \\
&= {\sigma_p}^{n-2}(\sigma_p(\alpha))^p = {\sigma_p}^{n-2}((\alpha^p)^p) = {\sigma_p}^{n-2}(\alpha^{p^2}) \\
&= \cdots = \alpha^{p^n} = \alpha
\end{aligned}$$

so ${\sigma_p}^n$ is the identity automorphism. If α is a generator of the group E^*, then $\alpha^{p^i} \neq \alpha$ for $i < n$, so we see that n is indeed the order of σ_p.

b. Section 33 shows that E is an extension of $\mathbb{Z}_p$ of order n, and is the splitting field of any irreducible polynomial of degree n in $\mathbb{Z}[x]$. Because E is a separable extension of the finite perfect field $\mathbb{Z}_p$, we see that $|G(E/F)| = \{E : F\} = [E : F] = n$. Since $\sigma_p \in G(E/F)$ has order n, we see $G(E/F)$ is cyclic of order n.

15. a. Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{i=0}^{\infty} b_i x^i$. Then

$$\begin{aligned}
D(f(x) + g(x)) &= D\left(\sum_{i=0}^{\infty}(a_i + b_i)x^i\right) \\
&= \sum_{i=1}^{\infty}(i \cdot 1)(a_i + b_i)x^{i-1} \\
&= \sum_{i=1}^{\infty}(i \cdot 1)a_i x^{i-1} + \sum_{i=1}^{\infty}(i \cdot 1)b_i x^{i-1} \\
&= D(f(x)) + D(g(x)).
\end{aligned}$$

thus D is a homomorphism of $\langle F[x], +\rangle$.

b. If F has characteristic zero, then $\mathrm{Ker}(D) = F$.

c. If F has characteristic p, then $\mathrm{Ker}(D) = F[x^p]$.