19 Show the following:

a. If $f \in F[t]$, $\operatorname{char} F = 0$, and the derivative $f' = 0$, show $f \in F$.

b. If $\operatorname{char} F = p \neq 0$, $f \in F[t]$, and $f' = 0$, then show there exists $g \in F[t]$ such that $f(t) = g(t^p)$.

Solution a. Write $f = a_n t^n + \cdots + a_1 t + a_0$. Then $0 = f' = na_n t^{n-1} + \cdots + a_1$. Because F has characteristic 0, this means that $ka_k = 0 \implies a_k = 0$, since F is a domain. Thus, $a_1 = \cdots = a_n = 0$, so $f = a_0 \in F$.

b. As before, $0 = f' = na_n t^{n-1} + \cdots + a_1$. Then $ka_k = 0$ means $a_k = 0$ or $k = 0$, i.e., $p \mid k$. Thus, the only possible non-zero coefficients are $a_0, a_p, a_{2p}, \ldots$, so

$$f = a_{rp}t^{rp} + a_{(r-1)p}t^{(r-1)p} + \cdots + a_0 = a_{rp}(t^p)^r + a_{(r-1)p}(t^p)^{r-1} + \cdots + a_0 = g(t^p),$$

where $g = a_{rp}t^r + \cdots + a_0$.

---

20 Show that if x is transcendental over F, then $t^2 - x \in F(x)[t]$ is irreducible.

Solution Suppose $t^2 - x$ is reducible, so that $(t-a)(t-b) = t^2 - x$, for some $a, b \in F(x)$. Then $a + b = 0$. Because x is transcendental, this means that $a = -b$.

Similarly, we get $x = -ab = a^2$. But a^2 is a polynomial $p(x)$ in x with even degree, which means that x is a root of the polynomial $p(t) - t \in F$, which is impossible, as x was transcendental. Thus, $t^2 - x$ must be irreducible.

---

21 Suppose that $\operatorname{char} F = p \neq 0$. Show the following:

a. The map $F \to F$ given by $x \mapsto x^p$ is a monomorphism. Denote its image by F^p.

b. If K/F is algebraic and $\alpha \in K$ is separable over $F(\alpha^p)$, then $\alpha \in F(\alpha^p)$.

c. Every finite field is perfect, i.e., every algebraic extension is separable.

Solution a. Denote the map by f. It is a homomorphism: $f(0) = 0^p = 0$, $f(1) = 1^p = 1$, $f(x+y) = (x+y)^p = x^p + y^p = f(x) + f(y)$, since F has characteristic p, and $f(xy) = (xy)^p = x^p y^p = f(x)f(y)$.

We now need to show that the map is an injection.

Let $x, y \in F$ be so that $x^p = y^p$. Then

$$(x-y)^p = x^p - y^p = 0 \implies x - y = 0 \implies x = y,$$

since fields are domains, so f is an injection.

b. Consider the polynomial $(t-\alpha)^p = t^p - \alpha^p \in F(\alpha^p)$. α is a root of this polynomial, which means that its minimal polynomial divides it. In particular, this means that its minimal polynomial is of the form $f = (t-\alpha)^k$ for some k. Since α is separable, f must have distinct roots, so $k = 1$, i.e., its minimal polynomial is $t - \alpha$. Since $f \in F(\alpha^p)$, it follows that $\alpha \in F(\alpha^p)$.

c. Let K/F be algebraic, but assume that there exists $\alpha \in K$ which is not separable. Let f be the minimal polynomial of α, so that $f(\alpha) = 0$, but f has multiple roots.

Since f has multiple roots, f' shares a non-trivial factor with f. But f is irreducible, which means that f divides f'. But the degree of f' is smaller than that of f, so $f' = 0$. Hence, by problem 19(b), $f(t) = g(t^p)$ for some

$$g = a_n t^n + \cdots + a_0 \in F[t].$$

But by (a), every element has a p-th root, so for each a_i, there exists b_i such that $b_i^p = a_i$, so

$$f(t) = b_n^p (t^n)^p + \cdots + b_0^p = (b_n t^n + \cdots + b_0)^p,$$

but f was irreducible, a contradiction. Hence, α must have been separable.

22 Suppose that $\operatorname{char} F = p \neq 0$. Show the following:

a. If K/F is separable, then $K = F(K^p)$.

b. Suppose that K/F is finite and $K = F(K^p)$. If $\{x_1, \ldots, x_n\} \subseteq K$ is linearly independent over F, then so is $\{x_1^p, \ldots, x_n^p\}$.

c. If K/F is finite and $K = F(K^p)$, then K/F is separable.

Solution a. "$\supseteq$" is clear, since $K^p \subseteq K$, so we just need to show "$\subseteq$".

Let $\alpha \in K$. By assumption, α is separable, and in particular it is algebraic. Thus, by 21(b), $\alpha \in F(\alpha^p) \subseteq F(K^p)$, which proves the equality.

b. Suppose there are $a_1, \ldots, a_n \in F$ so that $a_1 x_1^p + \cdots + a_n x_n^p = 0$. Since K/F is finite, F is also finite, so the map $x \mapsto x^p$ is an isomorphism. In particular, for each a_i, there exists $b_i \in F$ so that $b_i^p = a_i$, so

$$0 = a_1 x_1^p + \cdots + a_n x_n^p = b_1^p x_1^p + \cdots + b_n^p x_n^p = (b_1 x_1 + \cdots + b_n x_n)^p.$$

Since $K[t]$ is a domain, it follows that $b_1 x_1 + \cdots + b_n x_n = 0$, and by assumption, this means that $b_1 = \cdots = b_n = 0 \implies a_1 = \cdots = a_n = 0$, as desired.

c. Let $\alpha \in K/F$. Since K/F is finite, $\{1, \alpha, \alpha^2, \ldots\}$ cannot be linearly independent over F, so α must be algebraic. Let f be the minimal polynomial of α over F, with

$$f = a_n t^n + \cdots + a_0.$$

In particular, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is linearly independent.

Suppose f has a multiple root. Then because $\operatorname{char} F \neq 0$, $f' = 0$, so $f(t) = g(t^p)$ for some $g \in F[t]$, and so $g(\alpha^p) = 0$. But this is an equation in $\left\{1, \alpha^p, \ldots, \alpha^{(n-1)p}\right\}$, which is linearly independent over F by (b). But this implies that all the coefficients of g are 0, which in turn implies that f is the zero polynomial, which is impossible. Thus, f must have distinct roots.

---

23 Let K/F. Show the following:

a. If $\alpha \in K$ is separable over F, then $F(\alpha)/F$ is separable.

b. If $\alpha_1, \ldots, \alpha_n \in K$ are separable over F, then $F(\alpha_1, \ldots, \alpha_n)/F$ is separable.

c. Let $F_{\text{sep}} = \{\alpha \in K \mid \alpha \text{ separable over } F\}$. Then F_{sep} is a field.

Solution a. $F(\alpha)/F$ is finite, so by 22(c), it suffices to show that $F(\alpha) = F(\alpha^p)$. "$\supseteq$" is clear, so we just need to show the other direction.

By assumption, $F(\alpha)/F$ is algebraic and α is separable, so by 21(b), $\alpha \in F(\alpha^p)$, which proves equality. Hence, $F(\alpha)/F$ is separable.

b. Notice that α_2 is still separable over $F(\alpha_1)$ since it's just a field extension. Thus, $F(\alpha_1, \alpha_2)/F$ is separable. The result follows by induction on n.

c. 0 and 1 are certainly in F_{sep}; we can just consider the polynomials t and $t - 1$.

Now let $\alpha, \beta \in F_{\text{sep}}$. Then by (b) $F(\alpha, \beta)/F$ is separable, so $\alpha + \beta$, $\alpha\beta$, α^{-1}, etc., are separable as well, so F_{sep} is a field.

24 Show any algebraic extension of a perfect field is perfect.

Solution Let F be a perfect field and let K/F be an algebraic extension. By definition, for all algebraic $\alpha \in F$, α is the root of a separable polynomial over F.

Let α be an algebraic element of K. Since K/F is algebraic, α is algebraic in F, and hence is a root of a separable polynomial $f \in F[t] \subseteq K[t]$. Because f is separable in F, it is separable in K, which shows that K/F is perfect.

---

25 Let F_o be a field of characteristic $p > 0$, $F = F_o(t_1^p, t_2^p)$, and $L = F_o(t_1, t_2)$. Show the following:

a. If $\theta \in L \setminus F$, then $[F(\theta) : F] = p$.

b. There exist infinitely many fields K satisfying $F < K < L$.

Solution a. Write $\theta = a + p(t_1, t_2)$, there f is a polynomial. Then $\theta^p = a^p + f(t_1^p, t_2^p) \in F$, since $\operatorname{char} F_0 = p$. Thus, $(t-\theta)^p = t^p - \theta^p$ must be the minimal polynomial for θ over F. If $(t-\theta)^k \in F$ with $1 < k < \theta$, then this implies that $\theta^k \in F$, but this is impossible since k does not divide p unless θ is 1 or p.

Thus, $F(\theta) = F[t]/(t^p - \theta^p)$, so $[F(\theta) : F] = p$, as required.

b. We claim that $K = F(t_1 + \gamma t_2)$ works as γ varies over F_0. Indeed, $[L : F] = p^2$ by picking a basis, which means that $F < F(t_1 + \gamma t_2) < L$, as long as $t_1 + \gamma t_2 \in L \setminus F$, by (a). We just need to check that these give different field extensions:

Let $\mu \neq \gamma \in F$ be so that $t_1 + \gamma t_2, t_1 + \mu t_2 \notin F$. Suppose $F(t_1 + \gamma t_2) = F(t_1 + \mu t_2)$. Then

$$(\gamma - \mu)t_2 = t_1 + \gamma t_2 - (t_1 + \mu t_2) \in F(t_1 + \gamma t_2).$$

Thus, $t_2 \in F(t_1 + \gamma t_2)$, since we can just divide by $\gamma - \mu$. A similar calculation shows that $t_1 \in F(t_1 + \gamma t_2)$, but this means that $F(t_1 + \gamma t_2) = F(t_1, t_2)$, which is a contradiction, by problem 45. Hence, μ and γ must give different fields, which means that there are infinitely many intermediate fields.

---

43 Show that if F is a finite field, $n \in \mathbb{Z}^+$, then there exists an irreducible polynomial $f \in F[t]$ of degree n.

Solution We know that $|F| = q = p^m$, for some prime p and integer m. So, we will write $F = \mathbb{F}_q$.

Because $\mathbb{F}_{q^n}^\times$ is finite, it follows that it is a cyclic group, so let α be such that $\langle \alpha \rangle$. Notice then that $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$. Indeed, "$\subseteq$" is trivial, and "$\supseteq$" follows from the fact that α generates the non-zero elements of $\mathbb{F}_{q^n}$. Hence,

$$[\mathbb{F}_{q^n} : \mathbb{F}_q] = n.$$

In particular, the minimal polynomial f of α must have degree n, or else the degree of the extension cannot be n. In particular, f is irreducible and of degree n, which is what we wanted.

44 Show that if F is a finite field, then every element in F is a sum of two squares.

Solution $\operatorname{char} F = 2$:

In this case, consider the Frobenius endomorphism $\varphi\colon F \to F$, $\varphi(x) = x^2$. Then $\ker\varphi = \{0\}$, so φ is an injection. Because F is finite, φ is also surjective and so, for every $y \in F$, there exists x so that $y = x^2 + 0^2$, which proves the statement in this case.

$\operatorname{char} F > 2$:

We again consider the map $\varphi\colon F^\times \to F^\times$, $\varphi(x) = x^2$.

First, notice that if we have $x, y \in F$ so that $\varphi(x) = \varphi(y)$,

$$0 = x^2 - y^2 = (x - y)(x + y),$$

so $x = y$ or $x = -y$. Since $\operatorname{char} F > 2$, $y \neq -y$, which tells us that every element in the image $\varphi(F)$ comes from precisely two elements in F, i.e., there are

$$\frac{|F^\times|}{2} = \frac{|F| - 1}{2}$$

square elements in $F^\times$. If we include 0, this means that there are

$$\frac{|F| + 1}{2}$$

squares in F.

Let $x \in F$. Notice that because translation is injective,

$$\frac{|F| + 1}{2} = \big|\{a^2 \mid a \in F\}\big| = \big|\{x - a^2 \mid a \in F\}\big|.$$

Since $2 \cdot (|F| + 1)/2 = |F| + 1$, the pigeonhole principle tells us that the two sets cannot be disjoint, i.e., there exists $a, b \in F$ so that $a^2 = x - b^2 \implies x = a^2 + b^2$, which completes the proof.

---

45 Show that if F is not a finite field and u, v are algebraic and separable over K, then there exists an element $a \in K$ such that $K(u, v) = K(u + av)$. Is this true if $|K| < \infty$ with $K(u) < K(u, v)$ and $K(v) < K(u, v)$?

Solution Since u and v are algebraic, they both have minimal polynomials $m_F(u)$, $m_F(v)$, over F. Because they are separable, the roots of $m_F(u)$ and $m_F(v)$ are distinct, which we'll label as $u, u_1, \ldots, u_n$ and $v, v_1, \ldots, v_m$, respectively.

Pick a so that $u + av \neq u_i + av_j$, for all $1 \leq i \leq n$ and $1 \leq j \leq m$. Such an a exists because F is not finite and because all the roots are distinct; indeed, there are finitely many nm bad values of a.

To show that $K(u, v) = K(u + av)$, we just need to show that $v \in K(u + av)$, since this implies that $u = (u + av) - av \in K(u + av)$, which shows "$\subseteq$". On the other hand "$\supseteq$" is clear.

Consider $f(t) = m_F(u)((u + av) - at) \in K(u + av)[t]$. By construction, $f(v) = 0$, and no other v_i is a root of f, so $\gcd(f, m_b) = t - v$. Since the polynomial ring over a field is Euclidean domain, there exist $g, h \in K(u + av)[t]$ so that $gf + hm_b = t - v$. All of the coefficients of g and h are in $K(u + av)$, so it follows that $v \in K(u + av)$, as required.

It is not true in general if K is a finite field.