Question 1

Let F be a field of $\text{char}(F) = p$. Show that if $\gcd([K : F], p) = 1$, then K/F is separable.

Solution: Let $K_s = \{\, \alpha \mid \alpha \text{ is separable over } F \,\}$, then notice that by problem 10, K/K_s is purely inseparable. Then as K/F is finite, K/K_s is finite, but by problem 8, $[K : K_s]$ must be of p-power, so let $[K : K_s] = p^n$ Now, as $[K : F] = [K : K_s][K_s : F]$, it follows that $p^n \mid [K : F]$. However, as $\gcd([K : F], p) = 1$, then $n = 0$. Therefore, $[K : F] = [K_s : F]$, thus K/F must be separable.

Question 2

Let $f \in F[x]$ be a nonzero polynomial over a field F. Show that the polynomial $f/\gcd(f, f')$ is separable, where f' denotes the derivative of f.

Solution: If $f' = 0$, then $\gcd(f, f') = f$, and $f/\gcd(f, f') = 1$ is separable. Now assume $f' \neq 0$ Consider a field K/F such that f and f' are split in K, then let α be arbitrary root of f and n be the maximal number such that $(x-\alpha)^n \mid f$. Then, $f(x) = (x-\alpha)^n g(x)$ for some polynomial $g(x)$ over F. So,

$$0 \neq f'(x) = n(x-\alpha)^{n-1}g(x) + (x-\alpha)^n g'(x) = (x-\alpha)^{n-1}(ng(x) - (x-\alpha)g'(x))$$

As $(x-\alpha)^{n-1} \mid f'(x)$, then $(x-\alpha)^{n-1} \mid \gcd(f, f')$. Hence, α is a root of $f/\gcd(f, f')$ with multiplicity at most 1. Therefore, $f/\gcd(f, f')$ is separable.

Question 3

Show that a field F is perfect if and only if any finite extension of F is separable.

Solution:

($\Longrightarrow$):

If $\text{char}(F) = 0$, let f be an irreducible polynomial over F. Then, $f' \neq 0$ since if $\deg(f) > 1$, $\deg(f') \geq 1$ and if $\deg(f) = 1$, then $f = ax + b$, so $f' = a \neq 0$. Therefore, as $\deg(f') = \deg(f) - 1$ and $f' \neq 0$, and f is irreducible, it follows that $\gcd(f, f') = 1$. As $f' \neq 0$, f is separable. Therefore, all irreducible polynomial in $F[x]$ is separable.

If $\text{char}(F) = p$, then $f' = 0$ means $f = a_n x^{np} + \cdots + a_1 x^p + a_0$ since otherwise, if f contains some term bx^k where p does not divide k, then f' contains bkx^{k-1} where $bk \neq 0$. However, as F is perfect, for every a_i there exists b_i such that $b_i^p = a_i$. Therefore,

$$f = a_n x^{np} + \cdots + a_0 = b_n^p x^{np} + \cdots + b_0^p = (b_n x^n + \cdots + b_0)^p$$

Thus, f is not irreducible. Therefore, all irreducible polynomial in $F[x]$ is separable.

As all irreducible polynomial in F is separable, let E/F be a finite extension, thus algebraic. Then for any $\alpha \in E$, there exists m_α such that it is monic irreducible and $m_\alpha(\alpha) = 0$. Then, since m_α is irreducible, it is separable, thus α is separable.

($\Longleftarrow$):

Assuming that all finite extension of F is separable, let f be an irreducible polynomial over F and α is a root of f. Then, choose $E = F(\alpha)$ so that $[E : F] = \deg(f)$ is finite, thus E/F is separable. Therefore α is separable, so f separable.

Assuming that F is not perfect, which is that $\text{char}(F) = p$ and $F \neq F^p$. Choose $a \in F - F^p$ and construct a polynomial $f(x) = x^p - a$. Then, consider b in the splitting field of f over F such that b is the root of f. Then, $b^p = a$. Therefore, $f(x) = x^p - a = (x-b)^p$, which means that f is not separable.

Next, choose $E = F(b)$ so that $[E : F] \leq \deg(f) = p$ is finite, therefore, E is separable by assumption. This means that b is separable, which is that the minimal polynomial of b, say m_b must divides f and be separable. This leaves the only possibility of $m_b = (x-b)$ over F. So, $b \in F$. However, if $b \in F$, then $a = b^p \in F^p$ contradicting that $a \in F - F^p$.

Question 4

Show that every finite extension of a perfect field is perfect.

Solution: Let F be a perfect field and E/F a finite extension. Consider a finite extension K over E so that $K/E/F$ is an extension. Then, K/F is also a finite extension by the tower law. As F is perfect, K is separable. This was shown in the previous problem. As K is an arbitrary finite extension of E, then all finite extension of E is separable. So, E is perfect. This was also shown in the previous problem.

Question 5

Let F be a finite field and of characteristic 2. Show that if E/F is a separable extension of degree 2, then $E = F(\alpha)$ for some $\alpha \in E$ such that $\alpha^2 + \alpha \in F$.

Solution: As E/F is degree 2, then $E = F(\alpha)$ for some $\alpha \in E$. Moreover, there exists irreducible polynomial f of degree 2 such that $f(\alpha) = 0$. Since E/F is separable, then α must be separable, so f must be separable. This mean that $f = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta) + \alpha\beta$ for some $\beta \neq \alpha$. Thus, $\alpha\beta \in F$. Consider $e = f(\alpha\beta) = \alpha(\beta-1)\beta(\alpha-1)$ as an element in F. Then,

$$\frac{e}{\beta^2 - \beta} = \alpha(\alpha - 1) = \alpha^2 - \alpha = \alpha^2 + \alpha - 2\alpha = \alpha^2 + \alpha$$

So, $\alpha^2 + \alpha \in F$.

Question 6

Let F be a finite field and let $E = F(\alpha, \beta)/F$ be a finite extension. Show that if $F(\alpha) \cap F(\beta) = F$, then $E = F(\alpha + \beta)$

Solution: Let $F = \mathbb{F}_q$ for $q = p^r$ for some prime p. Then, $F(\alpha) \simeq \mathbb{F}_{q^n}$ and $F(\beta) \simeq \mathbb{F}_{q^m}$. Notice that $E = F(\alpha, \beta)$ is finite, thus any subfield of E of certain order is unique since the unique field of order q^l is the field of $\left\{ x \mid x^{q^l} - x = 0 \right\}$, which there are exactly q^l solutions. Then assume $d \mid n$ and $d \mid m$ for $d > 1$. This means that $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$ and $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^m}$. As $F(\alpha) \subset E$ and $F(\beta) \subset E$, the field $\mathbb{F}_{q^d}$ is the same, thus $F(\alpha) \cap F(\beta) = \mathbb{F}_{q^d} \neq F$. Therefore, it is acheived that $\gcd(n, m) = 1$.

Now, consider the minimal polynomial f of $\alpha + \beta$. Notice since $x^{q^d} - x$ is the product of all monic irreducible polynomial over $\mathbb{F}_q$, then if the degree of f is k, then $x^{q^k} - x$ is satisfied by $\alpha + \beta$. Moreover, since f is minimal, $x^{q^d} - x$ should not be satisfied by $\alpha + \beta$ for any $d < k$.

Assume that $(\alpha+\beta)^{q^d} - (\alpha+\beta) = 0$, then $(\alpha+\beta)^{q^d} = \alpha + \beta$. Then,

$$\alpha + \beta = (\alpha+\beta)^{q^{nd}} = \alpha^{q^{nd}} + \beta^{q^{nd}} = \alpha + \beta^{q^{nd}}$$

because $\alpha^{p^n} = \alpha$ Thus, $\beta = \beta^{q^{nd}}$. But since β is of degree m with $\gcd(n, m) = 1$, then $m \mid d$. Similarly, the same process for $(\alpha+\beta)^{q^{md}} = \alpha + \beta$ shows that $n \mid d$. Thus, d is at least nm. Moreover, $x^{q^{nm}} - x$ is satisfy by $\alpha + \beta$ as $\alpha + \beta$ is a member of $F(\alpha, \beta)$, which is of degree at most nm over F. This proves that $[F(\alpha+\beta) : F] = nm$ and $[F(\alpha, \beta) : F] = nm$, thus, $F(\alpha + \beta) = F(\alpha, \beta)$.

Question 7

Let E/F be a finite extension and $E_s = \{ \alpha \in E \mid \alpha \text{ is separable over } F \}$. Prove that E_s is a subfield of E containing F.

Solution: Consider that for any $a \in F$, the polynomial $(x - a)$ over F is irreducible and separable, thus $a \in F$ is separable over F. So $F \subset E_s$.

Note that for any set S of separable elements, $F(S)$ is separable, consider the proof by induction. If $|S| = 1$, then let $E_s = \{ \alpha \}$. It is clear that $F(\alpha)/F$ is separable as α is separable. Then, assume that the result holds for $|S| = n$. Then consider $\alpha \notin S$ such that α is separable. Since $F(S)$ is separable over F and $F(S)(\{ \alpha \})$ is separable over $F(S)$ as shown above (because $|\{ \alpha \}| = 1$). Then, $F(S + \{ \alpha \})$ is separable over F. Therefore, by induction, $F(S)$ is separable.

Next, notice that E_s is a set of separable elements and $F(E_s)$ is the smallest field containing E_s, the smallest field containing all separable elements. As E_s is a set of separable elements, then $F(E_s)$ is separable, so every element of $F(E_s)$ is separable over F, which is that $F(E_s) \subset E_s$ by definition of E_s. In other words, $E_s = F(E_s)$ is a subfield.

Question 8

Let E/F be a field of $\text{char}(F) = p$ and let E/F be a finite extension. An element $\alpha \in E$ is called purely inseparable over F if $\alpha^{p^n} \in F$ for some nonnegative integer n. We say that E/F is purely inseparable if all elements in E are purely inseparable over F. Show that E/F is purely inseparable if and only if E/L and L/F are purely inseparable. Deduce that a finite purely inseparable extension has p-power degree.

Solution:

($\Longrightarrow$):

Consider E/L and L/F. If α is any element in L, then $\alpha \in E$, so α is purely inseparable over F as E/F is purely inseparable. Thus, L/F is purely inseparable. Next, If $\alpha \in E$ is any element, then $\alpha^{p^n} \in F \subset L$ for some nonnegative n. Thus, α is purely inseparable over L. So, E/L is purely inseparable.

($\Longleftarrow$):

Let α be any element in E, then as E/L is purely inseparable, $\alpha^{p^n} \in L$ for some nonnegative n. Then as L/F is purely inseparable, $(\alpha^{p^n})^{p^m} \in F$ for some nonnegative m. But as

$$(\alpha^{p^n})^{p^m} = \alpha^{p^n \cdot p^m} = \alpha^{p^{n+m}}$$

where $n+m$ is a nonnegative integer, then, E/F is inseparable.

If $E = F$ is purely inseparable, then $[E : F] = 1 = p^0$ Next, if E/F is a finite purely inseparable extension with $E \neq F$ then for any element $\alpha \in E - F$ there is a polynomial $f(x) = (x^{p^n} - \alpha^{p^n})$ over F such that $f(\alpha) = 0$. Thus the minimal polynomial of α must divides f. As $f(x) = (x^{p^n} - \alpha^{p^n})$ over F of characteristic p, then

$$f(x) = (x-\alpha)^{p^n} = (x^p - \alpha^p)^{p^{n-1}} = \cdots = (x^{p^n} - \alpha^{p^n})$$

Note that any divisor of $f(x)$ must be in the above form, as for k that is not divisible by p,

$$(x-\alpha)^{kp^n} = (x^{p^n} - \alpha^{p^n})^k = x^{p^n k} \pm (k\alpha^{p^n}) x^{p^n(k-1)} + \cdots + \alpha^{p^n k}$$

If $\alpha^{p^n} \in F$, then $(x-\alpha)^{p^n}$ is already less degree than $(x-\alpha)^{kp^n}$ otherwise, $k\alpha^{p^n} \notin F$ since $\alpha^{p^n} \notin F$ but $0 \neq k \in F$.

Therefore, the minimal polynomial of α must be of degree p^k for some integer k. Since $E = F(\beta)$ for some element $\beta \in E$, the degree $[E : F] = \deg(m_\beta) = p^k$ for some integer k.

Question 9

Let E/F be a finite extension of a field F of $\text{char}(F) = p$. Prove that if $\alpha \in E$ is separable and purely inseparable over F, then $\alpha \in F$.

Solution: Let $\alpha \in E$ be separable and purely inseparable. Then $\alpha^{p^n} \in F$ for some nonnegative integer n. Then, consider the polynomial $f(x) = x^{p^n} - \alpha^{p^n}$ over F. Since $f(\alpha) = 0$, the minimal polynomial of α must divide f.

However as F is of characteristic p,

$$f = (x^{p^n} - \alpha^{p^n}) = (x-\alpha)^{p^n}$$

Since α is separable over F, then $m_\alpha = (x-\alpha)$ must hold. Since m_α is the minimal polynomial over F, then $-\alpha \in F$, which is that $\alpha \in F$.

Question 10

Let E/F be a finite extension of a field F of $\text{char}(F) = p$. Show that E/E_s is purely inseparable, where E_s is the subfield defined in problem 7.

Solution: Let α be any element in E. If α is separable, then choose $\alpha = \alpha^{p^0}$ is separable, thus α is purely inseparable. Otherwise, let f be the minimal polynomial of α. Note that f is irreducible and non-zero. As α is inseparable, $\gcd(f, f') \neq 1$, thus $f' = 0$ (because otherwise, $f \mid f'$).

In problem 3, and in fact, in class, it was shown that if $\text{char}(F) = p$, $f' = 0$ implies

$$f(x) = a_n x^{np} + \cdots + a_1 x^p + a_0 = g(x^{p^k})$$

for some non-zero polynomial g over F and some largest integer k such that $p^k \mid np$ for all n such that $a_n \neq 0$. This is due to the fact that if there is a term $a_m x^m$ with non-zero a_m and $p \nmid m$ in $f(x)$, then $f'(x) \neq 0$ as it contains the term ma_m where $m \neq 0$.

By choosing $g(x)$ in that way, there exists some term with non-zero coefficient x^m with $p \nmid m$ (because otherwise k is not maximized) in $g(x)$. Therefore, $g' \neq 0$. If g is reducible, say $g(x) = h_1(x)h_2(x)$, then

$$f(x) = g(x^{p^k}) = h_1(x^{p^k})h_2(x^{p^k})$$

contradicting that f irreducible, thus g is irreducible.

Since $\deg(g') < \deg(g)$ and g is irreducible, it follows that $\gcd(g, g') = 1$, because otherwise, $g \mid g'$. Now, as $\gcd(g, g') = 1$, g must be separable.

Now, notice that $g(\alpha^{p^k}) = f(\alpha) = 0$, so the minimal polynomial of α^{p^k} must divide g. However, as g is separable, α^{p^k} must be separable. This means that $\alpha^{p^k} \in E_s$, thus α is purely inseparable over E_s. As α is arbitrary, E/E_s is purely inseparable.