

Turn in problems 54, 55, 57, 58, 59, 60, 61, 62, 63, 64, 65.

Problem 54. If $f \in \mathbb{K}[X]$ (with \mathbb{K} field) has degree n and \mathbb{F} is a splitting field of f over \mathbb{K} , prove that $[\mathbb{F} : \mathbb{K}] \mid n!$.

Proof. If f has a degree 1 over \mathbb{K} , then it has only one zero a whose minimal polynomial must have degree 1. $1 = [\mathbb{K}(a) : \mathbb{K}] = [\mathbb{F} : \mathbb{K}] \mid 1!$. If f has degree 2 over \mathbb{K} , then it has at most two distinct zeros. Suppose f is reducible. Then it splits into two linear factors over \mathbb{K} and so $\mathbb{F} \cong \mathbb{K} \implies [\mathbb{F} : \mathbb{K}] = 1 \mid 2!$. Otherwise f is irreducible, and so the minimal polynomial for a zero a_1 of f must be of the form $\frac{f(x)}{\ell}$ for some $\ell \in \mathbb{K}$, and therefore both zeros a_1 and a_2 share the same minimal polynomial $x^2 + bx + c = (x - a_1)(x - a_2) \in \mathbb{K}[x]$. So then $x^2 - (a_1 + a_2)x + a_1a_2 = x^2 + bx + c \implies a_2 = -b - a_1 \in \mathbb{K}(a_1)$ and so $\mathbb{F} \cong \mathbb{K}(a_1) \implies [\mathbb{F} : \mathbb{K}] \in \{1, 2\}$ both of which divide $2!$. Suppose $[\mathbb{F} : \mathbb{K}] \mid d!$ if \mathbb{F} is the splitting field of any degree d polynomial f over \mathbb{K} for all $1 \leq d < m$ for some $m \geq 2$. Consider the statement for a degree m polynomial f over \mathbb{K} .

If f is reducible, then $f(x) = P(x)Q(x)$ for some non-constant degree p and $(m - p)$ polynomials P and Q over \mathbb{K} . Let \mathbb{F}_P be the splitting field of P over \mathbb{K} and \mathbb{F}_Q be the splitting field of Q over \mathbb{F}_P . Since $\deg_{\mathbb{K}}(P(x)) = p$, $\deg_{\mathbb{F}_P}(Q(x)) = \deg_{\mathbb{K}}(Q(x)) = m - p < m$, we have that $[\mathbb{F}_Q : \mathbb{F}_P] \mid (m - p)!$ and $[\mathbb{F}_P : \mathbb{K}] \mid p!$. Well, $\mathbb{F}_Q = (\mathbb{F}_P)(\alpha \mid Q(\alpha) = 0) \cong (\mathbb{K}(a \mid P(a) = 0))(b \mid Q(b) = 0) = \mathbb{K}(\alpha \mid P(\alpha) = 0 \text{ or } Q(\alpha) = 0) \cong \mathbb{F}$. So finally, $\mathbb{F}_Q \supseteq \mathbb{F}_P \supseteq \mathbb{K} \implies [\mathbb{F} : \mathbb{K}] = [\mathbb{F}_Q : \mathbb{K}] = [\mathbb{F}_Q : \mathbb{F}_P][\mathbb{F}_P : \mathbb{K}] \mid p!(m - p)! \mid m!$ (via $\binom{p}{m} = \frac{m!}{p!(m - p)!}$). So $[\mathbb{F} : \mathbb{K}] \mid m!$.

If f is irreducible, then for any zero a of f , $[\mathbb{K}(a) : \mathbb{K}] = m$ and by the division algorithm we have $f(x) = (x - a)Q(x)$ over $\mathbb{K}(a)$ where Q has degree $m - 1$. Since Q has degree less than m , the splitting field \mathbb{F}_Q of Q over $\mathbb{K}(a)$ must be such that $[\mathbb{F}_Q : \mathbb{K}(a)] \mid (m - 1)!$ and since $\mathbb{F}_Q = (\mathbb{K}(a))(\alpha \mid Q(\alpha) = 0) = \mathbb{K}(\alpha \mid x - \alpha = 0 \text{ or } Q(\alpha) = 0) \cong \mathbb{F}$ we have that $[\mathbb{F} : \mathbb{K}] = [\mathbb{F}_Q : \mathbb{K}] = [\mathbb{F}_Q : \mathbb{F}_P][\mathbb{F}_P : \mathbb{K}]$ divides $m(m - 1)! = m!$.

Thus, by induction,

If $\mathbb{F} \supseteq \mathbb{K}$ is the splitting field of a degree $n \in \mathbb{Z}^+$ polynomial over \mathbb{K} , then $[\mathbb{F} : \mathbb{K}] \mid n!$.

□

Problem 55. If $K \subseteq F$ is a field extension, F is algebraically closed, and E is the set of all elements of F that are algebraic over K , prove that E is an algebraic closure of K .

Problem 57. If $[F : K] = 2$, then $K \subseteq F$ is a normal extension.

Problem 58. If d is a nonnegative rational number, then $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d}))$ is the identity or is isomorphic to \mathbb{Z}_2 .

Problem 59. What is the Galois group of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over \mathbb{Q} ?

Problem 60. Assume K is a field of characteristic 0. Let G be the subgroup of $\text{Aut}_K(K(X))$ generated by the K -automorphism induced by $X \mapsto X + 1$. Prove that G is an infinite cyclic group. What is the fixed field E of G ? What is $[K(X) : E]$?

We prepare for the next problem by proving a bunch of useful stuff.

Lemma 1. *If \mathbb{K} is a field and $f(x) \in \mathbb{K}[x]$, $f(x)$ has some repeated zero α if and only if α is also a zero of $f'(x)$, the formal derivative of $f(x)$ over \mathbb{K} .*

Proof. (\implies) If α is a repeated zero of $f(x)$, then $f(x) = (x - \alpha)^2 g(x) \in \overline{\mathbb{K}}[x]$ for some $g(x)$ over an algebraic closure $\overline{\mathbb{K}}$ of \mathbb{K} . So then $f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x) \implies f'(\alpha) = 0$. (\impliedby) On the other hand if $f(\alpha) = f'(\alpha) = 0$, then $f(x) = (x - \alpha)q(x) \in \overline{\mathbb{K}}[x]$ for some $q(x)$ over $\overline{\mathbb{K}}$. Therefore, $f'(x) = q(x) + (x - \alpha)q'(x)$ and so $f'(\alpha) = q(\alpha) = 0 \implies q(\alpha) = 0$ since $q(x) = 0$ implies that $f(x) = 0$, a contradiction. So then $q(\alpha) = 0 \implies (x - \alpha) \mid q(x) \in \overline{\mathbb{K}}[x] \setminus \overline{\mathbb{K}} \implies f(x) = (x - \alpha)^2 h(x)$ for some $h(x) \in \overline{\mathbb{K}}[x]$ where $q(x) = (x - \alpha)h(x)$. So α is a repeated zero of $f(x)$. □

Theorem 2. \mathbb{K} is a finite field

$$\implies \text{Char } \mathbb{K} = p > 0 \text{ for some prime } p \quad (1)$$

$$\iff \mathbb{K} \text{ is some } n\text{-dimensional } \mathbb{k}_p\text{-vector space where } n \in \mathbb{Z}^+ \text{ and } \mathbb{k}_p \cong \mathbb{Z}_p \quad (2)$$

$$\iff \mathbb{K} \text{ is a splitting field of } f_{p,n}(x) = x^{(p^n)} - x \text{ over } \mathbb{k}_p \text{ where } n \in \mathbb{Z}^+ \text{ and } \mathbb{k}_p \cong \mathbb{Z}_p \quad (3)$$

Proof. (1) We can't have $\text{Char } \mathbb{K} = 0$ otherwise \mathbb{K} would be infinite, so $\text{Char } \mathbb{K} = p > 0$. Suppose p is not prime. (We typically just denote an n -sum of 1's $n := \sum_{i=1}^n 1$ in the context of our fields.) So $p = ab = 0$ for some $1 \leq a, b < p$. But then $p = ab = 0$ for some $a, b \neq 0$ and then \mathbb{K} has zero divisors, a contradiction. So $\text{Char } \mathbb{K} = p > 0$ for some prime p .

(2) (\implies) Since (1) $\implies \text{Char } \mathbb{K} = p > 0$ for some prime p , we have that $\mathbb{k}_p = \langle 1_{\mathbb{K}} \rangle_+ \cong \langle 1_{\mathbb{Z}_p} \rangle_+ = \mathbb{Z}_p$, a finite field because p is prime, via $1_{\mathbb{K}} \leftrightarrow 1_{\mathbb{Z}_p}$. So then $\mathbb{k}_p \subseteq \mathbb{K}$ is a subfield, and immediately by the field axioms we have that \mathbb{K} is a \mathbb{k}_p -vector space. Additionally, since \mathbb{K} is finite, it must also be finite dimensional over \mathbb{k}_p . Therefore, \mathbb{K} is an n -dimensional \mathbb{k}_p -vector space for some $n \in \mathbb{Z}^+$ and $\mathbb{k}_p \cong \mathbb{Z}_p$. (\impliedby) If \mathbb{K} is an n -dimensional \mathbb{k}_p -vector space where $n \in \mathbb{Z}^+$ and $\mathbb{k}_p \cong \mathbb{Z}_p$, then $|\mathbb{K}| = p^n$ and so \mathbb{K} is finite.

(3) (\implies) By (2) we have that $|\mathbb{K}| = p^n$ for some $n \in \mathbb{Z}^+$ and then for any $a \in \mathbb{K}^* = \mathbb{K} \setminus \{0\}$, the multiplicative group of \mathbb{K} , we have that $|a|$ divides $|\mathbb{K}^*| = p^n - 1$. Therefore, $a^{p^n-1} = 1 \implies a^{p^n} = a$. Therefore, every $a \in \mathbb{K}$ is a zero of $f_{p,n}(x) = x^{(p^n)} - x \in \mathbb{k}_p[x]$. Now, $f'_{p,n}(x) = p^n x^{p^n-1} - 1 = -1$ since $\text{Char } \mathbb{K} = p$ and so by **Lemma 1**, $f'_{p,n}(\alpha) = -1 \neq 0$ for all zeros α of $f_{p,n}(x) \implies f_{p,n}(x)$ has no repeated zeros. So then since $f_{p,n}(x)$ has at most p^n zeros which are all distinct, in fact \mathbb{K} must be exactly all distinct zeros of $f_{p,n}(x)$. Suppose $f_{p,n}(x)$ splits completely in a smaller field \mathbb{M} where $|\mathbb{M}| < |\mathbb{K}|$. But then $\mathbb{K} = \{\alpha \in \overline{\mathbb{K}} \mid f_{p,n}(\alpha) = 0\} \subseteq \mathbb{M} \implies |\mathbb{M}| \geq |\mathbb{K}|$ for some algebraic closure $\overline{\mathbb{K}}$ of \mathbb{K} , a contradiction. So then \mathbb{K} is a splitting field of $f_{p,n}(x)$ over \mathbb{k}_p . (\impliedby) If \mathbb{K} is a splitting field of $f_{p,n}(x) = x^{(p^n)} - x$ over $\mathbb{k}_p \cong \mathbb{Z}_p$, then it is generated by finitely many algebraic elements over \mathbb{k}_p which means it is algebraic over \mathbb{k}_p and therefore a finite extension of the finite field \mathbb{k}_p which means it is finite field itself. □

Now, we prepare some Corollaries.

Corollary 3. If \mathbb{K} is a finite field of characteristic $p > 0$, then inside a fixed algebraic closure $\overline{\mathbb{K}}$

$$\mathbb{k}_p = \langle 1 \rangle_+ \cong \mathbb{Z}_p \text{ is the prime subfield of } \mathbb{K} \quad (1)$$

$$\text{There exists a unique extension } \mathbb{K}_m \supseteq \mathbb{K} \text{ with } [\mathbb{K}_m : \mathbb{K}] = m \in \mathbb{Z}^+ \quad (2)$$

$$\text{There exists a unique subfield } \mathbb{k}_{p,d} \subseteq \mathbb{K} \text{ with } [\mathbb{k}_{p,d} : \mathbb{k}_p] = d \text{ for each divisor } d \text{ of } [\mathbb{K} : \mathbb{k}_p] \quad (3)$$

Proof. (1) Suppose there exists some subfield $\mathbb{M} \subseteq \mathbb{k}_p$ smaller than \mathbb{k}_p , so $|\mathbb{M}| < |\mathbb{k}_p|$. But then $0, 1 \in \mathbb{M} \implies \mathbb{k}_p = \langle 1 \rangle_+ \subseteq \mathbb{M} \implies |\mathbb{M}| \geq |\mathbb{k}_p|$, a contradiction. So \mathbb{k}_p must be the prime subfield of \mathbb{K} .

(2) By **Theorem 2.**, \mathbb{K} has dimension n over \mathbb{k}_p for some $n \in \mathbb{Z}^+$. Now, for some $m \in \mathbb{Z}^+$ let $f_{p,n,m}(x) = x^{(p^n)^m} - x \in \mathbb{K}_p$ and $\mathbb{K}_m = \{\alpha \in \overline{\mathbb{K}} \mid f_{p,n,m}(\alpha) = 0\}$. Observe.

For any $\alpha, \beta \in \mathbb{K}_m$ with $\beta \neq 0$, $f_{p,n,m}(\alpha - \beta) = (\alpha - \beta)^{p^{nm}} - (\alpha - \beta) = (\sum_{i=0}^{p^{nm}} \binom{p^{nm}}{i} \alpha^{p^{nm}-i} (-\beta)^i) - (\alpha - \beta) = (\alpha^{p^{nm}} + (-\beta)^{p^{nm}}) - (\alpha - \beta)$ since $\binom{p^{nm}}{0} = \binom{p^{nm}}{p^{nm}} = 1$ and $p \mid \binom{p^{nm}}{i}$ for all $0 < i < p^{nm}$ (I am uninterested in proving this part.) and since $p = 0$ we get that in fact $f_{p,n,m}(\alpha - \beta) = (\alpha^{p^{nm}} - \beta^{p^{nm}}) - (\alpha - \beta) = \alpha - \beta - (\alpha - \beta) = 0$. Note that this holds for $p = 2$ since $-\alpha = \alpha$ in a field with characteristic 2. Therefore, $\alpha - \beta \in \mathbb{K}_m$. Next, $f_{p,n,m}(\alpha\beta^{-1}) = (\alpha\beta)^{p^{nm}} = \alpha^{p^{nm}}\beta^{-p^{nm}} - (\alpha\beta^{-1}) = \alpha(\beta^{p^{nm}})^{-1} - \alpha\beta^{-1} = \alpha(\beta)^{-1} - \alpha\beta^{-1} = 0 \implies \alpha\beta^{-1} \in \mathbb{K}_m$.

So \mathbb{K}_m is a subfield of $\overline{\mathbb{K}}$ in which $f_{p,n,m}(x)$ splits completely. Suppose there is a smaller such field \mathbb{M} that $f_{p,n,m}(x)$ splits completely over, so $|\mathbb{M}| < |\mathbb{K}_m|$. But then $\mathbb{K}_m = \{\alpha \in \overline{\mathbb{K}} \mid f_{p,n,m}(\alpha) = 0\} \subseteq \mathbb{M} \implies |\mathbb{M}| \geq |\mathbb{K}_m|$, a contradiction. So \mathbb{K}_m must be a splitting field of $f_{p,n,m}(x)$ over \mathbb{k}_p . Finally, $a^{(p^n)} = a$ for all $a \in \mathbb{K}$. Suppose that for any $a \in \mathbb{K}$, $a^{(p^n)^c} = a$ for some $c \geq 1$. Then, $a^{(p^n)^{c+1}} = (a^{(p^n)^c})^{p^n} = (a)^{p^n} = a$. Therefore, by induction $a^{(p^n)^c} = a$ for all $c \geq 1$. So then every element $a \in \mathbb{K}$ is a zero of $f_{p,n,m}(x) = x^{(p^n)^m} - x$ and $\mathbb{K}_m \supseteq \mathbb{K} \supseteq \mathbb{k}_p$. So then we have $[\mathbb{K}_m : \mathbb{k}_p] = [\mathbb{K}_m : \mathbb{K}][\mathbb{K} : \mathbb{k}_p] = nm = [\mathbb{K}_m : \mathbb{K}]n \implies [\mathbb{K}_m : \mathbb{K}] = m$. Suppose some other distinct extension $\mathbb{E}_m \supseteq \mathbb{K}$ of degree m over \mathbb{K} exists. Well, it has order p^{nm} and all of its elements must be zeros of $f_{p,n,m}(x)$ via $|\mathbb{E}_m^*| = p^n - 1$, and then since $\mathbb{K}_m - \mathbb{E}_m \neq \emptyset$ we have that $|\mathbb{K}_m \cup \mathbb{E}_m| > p^{nm}$ and so $f_{p,n,m}(x)$ has more than p^{nm} distinct zeros, a contradiction. So \mathbb{K}_m is the unique extension with $[\mathbb{K}_m : \mathbb{K}] = m$ with respect to the closure $\overline{\mathbb{K}}$.

(3) By (2), we immediately get that there exists a unique extension $\mathbb{k}_{p,d} \supseteq \mathbb{k}_p$ with $[\mathbb{k}_{p,d} : \mathbb{k}_p] = d$ for each divisor $d \mid n$ which is a splitting field for $f_{p,m,d}(x) = x^{p^d} - x$ over \mathbb{k}_p . For any such divisor $d \mid n$, $a^{p^d} = a$ for all $a \in \mathbb{k}_{p,d}$. So then since $d \mid n$, $n = dq$ for some $q \in \mathbb{Z}^+$ and therefore by the induction earlier replacing \mathbb{K} with $\mathbb{k}_{p,d}$ we get that $a^{p^n} = a^{p^{dq}} = a$ for all $a \in \mathbb{k}_{p,d}$. Therefore every element in $\mathbb{k}_{p,d}$ is a zero of $f_{p,n}(x) = x^{p^n} - a$ over \mathbb{k}_p , and since \mathbb{K} is a splitting field for $f_{p,n}(x)$ in fact we have that $\mathbb{K} \supseteq \mathbb{k}_{p,d} \supseteq \mathbb{k}_p$. So then for each divisor $d \mid n$, $\mathbb{k}_{p,d}$, the splitting field of $f_{p,d}$ over \mathbb{k}_p , is a unique subfield of \mathbb{K} with $[\mathbb{k}_{p,d} : \mathbb{k}_p] = d$.

□

Alright now let's do the problem. I just wanted to prove this all myself instead of looking over the notes.

Problem 62. Let k be a finite field of characteristic $p > 0$.

- (a) Prove that for every $n > 0$ there exists an irreducible polynomial $f \in k[X]$ of degree n .
- (b) Prove that for every irreducible polynomial $P \in k[X]$ there exists $n \geq 0$ such that P divides $X^{p^n} - X$.

Proof. Fix some algebraic closure $\overline{\mathbb{K}} \supseteq \mathbb{K}$. Every object that follows is contained in $\overline{\mathbb{K}}$. By our theorems, if \mathbb{K} is a finite field of characteristic $p > 0$, p is prime and \mathbb{K} is an n -dimensional $\langle 1 \rangle_+ = \mathbb{k}_p$ -vector space for some $n \in \mathbb{Z}^+$. Also, there exists a unique extension \mathbb{K}_m of \mathbb{K} with $[\mathbb{K}_m : \mathbb{K}] = m$ for each $m \in \mathbb{Z}^+$. Finally, both \mathbb{K} and \mathbb{K}_m are unique splitting fields of $f_{p,n} = x^{p^n} - x$ and $f_{p,n,m} = x^{p^{nm}} - x$, respectively, over \mathbb{k}_p with respect to $\overline{\mathbb{K}}$. Suppose that for all $\alpha \in \mathbb{K}_m$, the degree of α over \mathbb{K} is strictly less than $[\mathbb{K}_m : \mathbb{K}] = m$. Any α must belong to $\mathbb{K}(\alpha) \subseteq \mathbb{K}_m$ and $[\mathbb{K}(\alpha) : \mathbb{K}] = d$ for some divisor $0 < d < nm$ of $[\mathbb{K}_m : \mathbb{k}_p] = nm$. Well, by our theorems this must be the unique subfield $\mathbb{k}_{p,d}$ of order p^d . Therefore,

$$\mathbb{K}_m = \bigcup_{\substack{d|nm \\ 0 < d < nm}} \mathbb{k}_{p,d} \implies |\mathbb{K}_m| = p^{nm} = \left| \bigcup_{\substack{d|nm \\ 0 < d < nm}} \mathbb{k}_{p,d} \right| \leq \sum_{\substack{d|nm \\ 0 < d < nm}} p^d < \sum_{i=0}^{nm-1} p^i = \frac{p^{nm} - 1}{1 - p} < p^{nm},$$

a contradiction. (Another contradiction is just the fact that then every $\alpha \in \mathbb{K}_m$ belongs to $\mathbb{k}_{p,d}$ for the largest $d < nm$ that divides nm and is less than m , but $|\mathbb{K}_m|$ is strictly less than p^{nm} . We did not prove directly that all these subfields are nested, so I didn't do that.) Therefore, there exists an element $\alpha_m \in \mathbb{K}_m$ with degree m over \mathbb{K} , and so there exists a monic irreducible polynomial of α_m over \mathbb{K} with degree m , that is $\mathbb{K}_m = \mathbb{K}(\alpha_m)$.

Now, consider any irreducible polynomial $P(x) \in \mathbb{K}[x]$. It must have some degree $q \in \mathbb{Z}^+$, and some zero α with the minimal polynomial $P_\alpha(x) = \frac{P(x)}{a} \in \mathbb{K}[x]$ where $a \in \mathbb{K}$ is the leading coefficient of $P(x)$. So then α has degree q over \mathbb{K} and $[\mathbb{K}(\alpha) : \mathbb{K}] = q$. Therefore, by our theorems, $\mathbb{K}(\alpha) = \mathbb{K}_q \subseteq \overline{\mathbb{K}}$, the splitting field of $f_{p,n,q}(x) = x^{p^{nq}} - x$ over \mathbb{k}_p . Well, $\alpha \in \mathbb{K}_q \implies |\alpha|$ divides $|\mathbb{K}_q^*| = p^{nq} - 1$ and so $\alpha^{p^{nq}-1} = 1 \implies \alpha^{p^{nq}} = \alpha \implies f_{p,n,q}(\alpha) = (\alpha)^{p^{nq}} - \alpha = 0$. So α is a zero of $f_{p,n,q}(x) = x^{p^{nq}} - x$ over \mathbb{k}_p , which is also a polynomial over \mathbb{K} .

□

Problem 63. Let p be a prime and \mathbb{F}_q (with $q = p^s$) be the finite field with q elements. Let $f \in \mathbb{F}_q[X]$ be an irreducible polynomial. Prove that f is irreducible in $\mathbb{F}_{q^m}[X]$ if and only if m and $\deg f$ are relatively prime.

Proof. Let $f(x)$ be an irreducible polynomial over \mathbb{F}_{p^n} with degree $\deg f(x) = d$ for some prime p and some $n \in \mathbb{Z}^+$. Also, let $f_{p,N}(x) = x^{p^N} - x$ over \mathbb{F}_p for any $N \in \mathbb{Z}^+$ and recall that every element of $\mathbb{F}_{p^{nN}}$, the splitting field of $f_{p,N}(x)$, is a zero of $f_{p,N}(x)$.

Now, since $f(x)$ is irreducible over \mathbb{F}_{p^n} , any zero α of $f(x)$ has the minimal polynomial $p_\alpha(x) = \frac{f(x)}{c}$ over \mathbb{F}_{p^n} where c is the leading coefficient of $f(x)$ and so it has degree d over \mathbb{F}_{p^n} . That is, $\mathbb{F}_{p^n}(\alpha) = \mathbb{F}_{p^{nd}}$. So then α is a zero of $f_{p,nd}(x)$, and we have that $\alpha^{p^{nd}} = \alpha$.

(\implies) Suppose $f(x)$ is irreducible over $\mathbb{F}_{p^{nm}}$, that is, every zero of $f(x)$ does not belong to $\mathbb{F}_{p^{nm}}$. Then, since $\mathbb{F}_{p^{nm}}$ is a splitting field for $f_{p,nm}(x)$, α must not be a zero of $f_{p,nm}(x)$. Suppose $\deg f(x) = d$ and m are not relatively prime. Then they share some divisor $q \geq 2$ such that $d = qa$ and $m = qb$ for some $a, b \in \mathbb{Z}^+$. Observe.

$$\alpha^{nd} = \alpha^{nqa} = \alpha \implies \alpha = \alpha^{nqab} = \alpha^{nma}$$

□

Problem 64. Prove that $E = \mathbb{F}_2[X]/(X^4 + X^3 + 1)$ is a field with 16 elements. What are the roots of $X^4 + X^3 + 1$ in E ?

Problem 65. Prove that an algebraic extension of a perfect field is a perfect field.

Problem 66. Show that the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$ is Galois. Find its Galois group.