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 $1 = [\mathbb{K}(a) : \mathbb{K}] = [\mathbb{F} : \mathbb{K}] \mid 1!$. If f has degree 2 over $\mathbb{K}$, then it has at most two distinct zeros. Suppose f is redicuble. 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 $x^2 - (a_1 + a_2)x + a_1 a_2 = x^2 + bx + c \implies a_2 = -b - a_1 \in \mathbb{K}(a)$ and so $\mathbb{F} \cong \mathbb{K}(a) \implies [\mathbb{F} : \mathbb{K}] \in \{1, 2\}$ 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 $[\mathbb{F}_Q : \mathbb{F}_P] \mid (m - p)!$ an $[\mathbb{F}_P : \mathbb{K}] \mid p!$. 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,

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

□

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

Proof. All elements of $\mathbb{E} = \{\alpha \in \mathbb{F} \mid \alpha \text{ is algebraic over } \mathbb{K}\}$ are algebraic over $\mathbb{K}$. Now, consider some polynomial $f(x)$ over $\mathbb{K}$. $\mathbb{F} \supseteq \mathbb{K} \implies \mathbb{F}[x] \supseteq \mathbb{K}[x] \implies f(x) \in \mathbb{F}$ and since $\mathbb{F}$ is algebraically closed, any zero a of $f(x)$ must belong to $\mathbb{F}$. So any algebraic a over $\mathbb{K}$ belongs to $\{\alpha \in \mathbb{F} \mid \alpha \text{ is algebraic over } \mathbb{K}\} = \mathbb{E}$.

Next, we prove that $\mathbb{E}$ is a field. For any $\alpha, \beta \in \mathbb{E} \subseteq \mathbb{F}$ with $\beta \neq 0$,

$$\begin{aligned}
&\alpha\beta^{-1}, \alpha - \beta \in \mathbb{K}(\alpha, \beta) \implies \mathbb{K}(\alpha, \beta, \alpha\beta^{-1}) = \mathbb{K}(\alpha, \beta, \alpha - \beta) = \mathbb{K}(\alpha, \beta) \\
&\implies \mathbb{Z}^+ \ni [\mathbb{K}(\alpha, \beta) : \mathbb{K}] = [\mathbb{K}(\alpha, \beta, \alpha\beta^{-1}) : \mathbb{K}(\alpha\beta^{-1})][\mathbb{K}(\alpha\beta^{-1}) : \mathbb{K}] \\
&\implies \mathbb{Z}^+ \ni [\mathbb{K}(\alpha, \beta) : \mathbb{K}] = [\mathbb{K}(\alpha, \beta, \alpha - \beta) : \mathbb{K}(\alpha - \beta)][\mathbb{K}(\alpha - \beta) : \mathbb{K}] \\
&\implies [\mathbb{K}(\alpha\beta^{-1}) : \mathbb{K}], [\mathbb{K}(\alpha - \beta) : \mathbb{K}] \in \mathbb{Z}^+
\end{aligned}$$

Therefore, since adjoining $\alpha\beta^{-1}$ or $\alpha - \beta$ to $\mathbb{K}$ gives a finite extension of K, they must algebraic over $\mathbb{K}$, and so they both belong to $\mathbb{E}$, which is then a subfield of $\mathbb{F}$. Additionally, since every element of $\mathbb{E}$ is algebraic over $\mathbb{K}$, $\mathbb{E}$ is an algebraic extension of $\mathbb{K}$. Lastly, consider any $g(x) = \sum_{i=0}^{n} \alpha_i x^i \in \mathbb{E}[x]$. Since $\mathbb{E}$ is algebraic over $\mathbb{K}$, $\alpha_0, \ldots, \alpha_n$ are all algebraic over $\mathbb{K}$. So then any zero β of $g(x)$ is algebraic over $\mathbb{K}(\alpha_0, \ldots, \alpha_n)$, which must be a finite extension of $\mathbb{K}$. Observe.

$$\begin{aligned}
&\mathbb{K}(\alpha_0, \ldots, \alpha_n, \beta) \supseteq \mathbb{K}(\beta) \supseteq \mathbb{K} \text{ and } [\mathbb{K}(\alpha_0, \ldots, \alpha_n, \beta) : \mathbb{K}(\alpha_0, \ldots, \alpha_n)] \in \mathbb{Z}^+ \\
&\implies [\mathbb{K}(\alpha_0, \ldots, \alpha_n, \beta) : \mathbb{K}] = [\mathbb{K}(\alpha_0, \ldots, \alpha_n, \beta) : \mathbb{K}(\alpha_0, \ldots, \alpha_n)][\mathbb{K}(\alpha_0, \ldots, \alpha_n) : \mathbb{K}] \in \mathbb{Z}^+ \\
&\implies \mathbb{Z}^+ \ni [\mathbb{K}(\alpha_0, \ldots, \alpha_n, \beta) : \mathbb{K}] = [\mathbb{K}(\alpha_0, \ldots, \alpha_n, \beta) : \mathbb{K}(\beta)][\mathbb{K}(\beta) : \mathbb{K}]
\end{aligned}$$

So $[\mathbb{K}(\beta) : \mathbb{K}] \in \mathbb{Z}^+ \implies \beta$ is algebraic over $\mathbb{K}$. Therefore, $\beta \in \mathbb{E}$ and $\mathbb{E}$ is an algebraically closed, algebraic extension of $\mathbb{K}$. Thus,

$$\mathbb{E} \text{ is an algebraic closure of } \mathbb{K}.$$

□

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

Proof. Let $P(x)\in\mathbb{K}[x]$ be irreducible over $\mathbb{K}$ with a zero $\alpha\in\mathbb{F}$. The minimal polynomial $P_\alpha(x)\in\mathbb{K}[x]$ of α must divide $P(x)$, and since $P(x)$ is irreducible over $\mathbb{K}$, $P_\alpha(x)=\frac{1}{c}P(x)$, where c is the leading coefficient of $P(x)$. Well, $\alpha\in\mathbb{F}\implies\mathbb{F}\supseteq\mathbb{K}(\alpha)\supseteq\mathbb{K}$. Therefore,

$$[\mathbb{F}:\mathbb{K}]=[\mathbb{F}:\mathbb{K}(\alpha)][\mathbb{K}(\alpha):\mathbb{K}]=2\implies\alpha\text{ has degree 1 or 2 over }\mathbb{K}.$$

If α has degree 1 over $\mathbb{K}$, $P_\alpha(x)$ and therefore $P(x)$ has only one zero, α which belongs to $\mathbb{F}$. If α has degree 2 over $\mathbb{K}$, then $P_\alpha(x)$ and therefore $P(x)$ has at most two distinct roots α,β such that $P_\alpha(x)=x^2+bx+c=(x-\alpha)(x-\beta)$. for some $b,c\in\mathbb{K}$. So then $x^2+bx+c=(x-\alpha)(x-\beta)=x^2-(\beta+\alpha)x+\alpha\beta=x^2+bx+c$. Finally, $\beta+\alpha=-b\implies\beta=b-\alpha\in\mathbb{F}$. In either case, $P(x)$ splits completely over $\mathbb{F}$. So then any irreducible polynomial over $\mathbb{K}$ with a root in $\mathbb{F}$ splits completely over $\mathbb{F}$.

Thus,

$$\text{If }[\mathbb{F}:\mathbb{K}]=2,\text{ then }\mathbb{K}\subseteq\mathbb{F}\text{ is a normal extension.}$$

□

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

Proof. If $\sqrt{d} \in \mathbb{Q}$, then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$ and so the only automorphism of $\mathbb{Q}$ that fixes $\mathbb{Q}$ is the identity, that is, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d})) = \{\mathrm{id}\} \cong \{e\}$. If $\sqrt{d} \notin \mathbb{Q}$, then it's minimal polynomial must be $x^2 - d \in \mathbb{Q}[x]$, and so it's only conjugate roots are $\sqrt{d}, -\sqrt{d}$. Any automorphism in $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d}))$ is completely defined by where it's adjoined root $\sqrt{d}$ is sent to, and since it may only be sent to it's conjugates $\sqrt{d}, \sqrt{-d}$ via $\mathrm{id} := \sqrt{d} \mapsto \sqrt{d}$ and $\phi := \sqrt{d} \mapsto -\sqrt{d}$, respectively, we have that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d})) = \{\mathrm{id}, \phi\} \cong \mathbb{Z}_2$.

Thus,

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

□

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

Proof. By the previous proof, $d \in \mathbb{Q} \setminus \mathbb{Q}^-$ and $\sqrt{d} \notin \mathbb{Q} \implies \sqrt{d}, -\sqrt{d}$ are the only conjugate roots of $\sqrt{d}$ over $\mathbb{Q}$. So then since any automorphism in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$ is completely defined by which conjugates over $\mathbb{Q}$ it's adjoined roots are permuted to, and each root has two conjugates, we have that $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})| = 2^3 = 8$. Let $\phi_d \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$ be the automorphism that sends $\sqrt{d}$ to $-\sqrt{d}$ and fixes all other roots, for each $d \in \{2,3,5\}$.

Any such ϕ_d^2 sends $\sqrt{d}$ to $-\sqrt{d}$ and then back to $\sqrt{d}$, and since it fixes everything else $\phi_d^2 = \mathrm{id}$ for each $d \in \{2,3,5\}$. By definition, these are distinct automorphisms which must generate the group, that is, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q}) = \langle \phi_2, \phi_3, \phi_5 \rangle$. Well, $\phi_a \circ \phi_b \coloneqq \begin{smallmatrix} \sqrt{a}\mapsto -\sqrt{a} \\ \sqrt{b}\mapsto -\sqrt{b} \end{smallmatrix} = \phi_b \circ \phi_a$ for each distinct pair $a,b \in \{2,3,5\}$, since these automorphisms don't affect generators other than the one, regardless of order. So then since all generators of the group commute pairwise, they all commute with each other in general and we have that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$ is an abelian group of order 8 with three distinct elements of order 2.

Thus,

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

□

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

Proof. Let $\phi \in \mathrm{Aut}_{\mathbb{K}}\big(\mathbb{K}(x)\big)$ be the $\mathbb{K}$-automorphism defined above, so $G = \langle \phi \rangle$. Now suppose G is finite of order $n \in \mathbb{Z}^+$. Then, $\phi^n := x \mapsto x+n = \mathrm{id} := x \mapsto x$, that is, $n = 0$ over $\mathbb{K}$. In fact since $|G| = n$, $k \neq 0$ for all $0 < k < n$. But then $\mathrm{Char}\ \mathbb{K} = n \in \mathbb{Z}^+$, a contradiction. So G must be an infinite cyclic group.

By definition, $\mathbb{E} = \mathrm{Fix}_{\mathbb{K}(x)}(G) = \{\frac{f(x)}{g(x)} \in \mathbb{K}(x) \mid \sigma(\frac{f(x)}{g(x)}) = \alpha,\ \forall \sigma \in G\}$. Consider any $Q(x) = \frac{f(x)}{g(x)} \in \mathbb{K}(x)$ which is fixed by G where $f(x), g(x)$ have $k, c \in \mathbb{N}$ distinct zeros over $\mathbb{K}$, respectively. (The base field $\mathbb{K}$ is always fixed by any subset of $\mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$ where $\mathbb{E}$ is an extension of $\mathbb{K}$, so this is an assumption we can make.) Then $Q(x)$ has at most k zeros and at most c poles.

Suppose $Q(x)$ has a zero $\alpha \in \overline{\mathbb{K}}$, for some fixed algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$, we must have that $Q(\alpha) = \phi^k(\alpha) = Q(\alpha + k) = 0$, $\forall k \geq 1$, and so Q has infinitely many zeros in $\overline{\mathbb{K}}$, a contradiction. So $Q(x)$ must not have any zeros. Next, notice that if $Q(x)$ is fixed by G, then so is $Q^{-1}(x) = \frac{g(x)}{f(x)}$. So then suppose $Q(x)$ has some pole $\beta \in \overline{\mathbb{K}}$. It is a zero of $Q^{-1}(x)$. But then once again we have that $Q^{-1}(\beta) = \phi_k(Q^{-1}(\beta)) = Q^{-1}(\beta + k) = 0$, $\forall k \geq 1$, and so $Q^{-1}(x)$ infinitely many poles in $\overline{\mathbb{K}}$, a contradiction. So then $Q(x)$ must have no poles.

Therefore, since $Q(x)$ has no poles or zeros, it must be some quotient which belongs to $\mathbb{K}$. So $\mathbb{E} \subseteq \mathbb{K}$. On the other hand, $G \subseteq \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}(x))$ fixes $\mathbb{K}$ by definition, so $\mathbb{K} \subseteq \mathbb{E}$. Therefore, $\mathbb{E} = \mathbb{K}$ is the fixed field of G. and since $\mathbb{E} = \mathbb{K}$, we must have that $K(x)$ has infinite dimension over $\mathbb{E} = \mathbb{K}$.

□

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*

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

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

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

Proof. (1) We can't have Char $\mathbb{K} = 0$ otherwise $\mathbb{K}$ would be infinite, so Char $\mathbb{K} = p > 0$. Suppose p is not prime. (We typically just denote an n-sum of 1's $n \coloneqq \sum_{i=1}^{n}$ 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 Char $\mathbb{K} = p > 0$ for some prime p.

(2) ($\implies$) Since (1) $\implies$ 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 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 $\overline{\mathbb{K}}$*

$$\Bbbk_p = \langle 1 \rangle_+ \cong \mathbb{Z}_p \text{ is the prime subfield of } \mathbb{K} \tag{1}$$

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

$$\text{There exists a unique subfield } \Bbbk_{p,d} \subseteq \mathbb{K} \text{ with } [\Bbbk_{p,d} : \Bbbk_p] = d \text{ for each divisor } d \text{ of } [\mathbb{K} : \Bbbk_p] \tag{3}$$

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

(2) By **Theorem 2.**, $\mathbb{K}$ has dimension n over $\Bbbk_p$ 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 $\beta \neq 0$, $f_{p,n,m}(\alpha - \beta) = (\alpha - \beta)^{p^{nm}} - (\alpha - \beta) = (\sum_{i=0}^{p^{mn}} \binom{p^{nm}}{i} \alpha^{p^{mn}-i}(-\beta)^i) - (\alpha - \beta) = (\alpha^{p^{mn}} + (-\beta)^{p^{mn}}) - (\alpha - \beta)$ since $\binom{p^{mn}}{0} = \binom{p^{mn}}{p^{mn}} = 1$ and $p \mid \binom{p^{nm}}{i}$ for all $0 < i < p^{mn}$ (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, $f_{p,n,m}(\alpha\beta^{-1}) = (\alpha\beta)^{p^{mn}} = \alpha^{p^{nm}}\beta^{-p^{nm}} - (\alpha\beta^{-1}) = \alpha(\beta^{p^{mn}})^{-1} - \alpha\beta^{-1} = \alpha(\beta)^{-1} - \alpha\beta^{-1} = 0 \implies \alpha\beta^{-1} \in \mathbb{K}_m$.

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 $\Bbbk_p$. 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 $\mathbb{K}_m \supseteq \mathbb{K} \supseteq \Bbbk_p$. So then we have $[\mathbb{K}_m : \Bbbk_p] = [\mathbb{K}_m : \mathbb{K}][\mathbb{K} : \Bbbk_p] = nm = [\mathbb{K}_m : \mathbb{K}]n \implies [\mathbb{K}_m : \mathbb{K}] = m$. 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 it's 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 $f_{n,p,m}(x)$ 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 $\Bbbk_{p,d} \supseteq \Bbbk_p$ with $[\Bbbk_{p,d} : \Bbbk_p] = d$ for each divisor $d|n$ which is a splitting field for $f_{p,m,d}(x) = x^{p^d} - x$ over $\mathbb{K}_p$. For any such divisor $d|n$, $a^{p^d} = a$ for all $a \in \Bbbk_{p,d}$. So then since $d|n, n = dq$ for some $q \in \mathbb{Z}^+$ and therefore by the induction earlier replacing $\mathbb{K}$ with $\Bbbk_{p,d}$ we get that $a^{p^n} = a^{p^{dq}} = a$ for all $a \in \Bbbk_{p,d}$. Therefore every element in $\Bbbk_{p,d}$ is a zero of $f_{p,n}(x) = x^{p^n} - a$ over $\Bbbk_p$, and since $\mathbb{K}$ is a splitting field for $f_{p,n}(x)$ in fact we have that $\mathbb{K} \supseteq \Bbbk_{p,d} \supseteq \Bbbk_p$. So then for each divisor $d \mid n$, $\Bbbk_{p,d}$, the splitting field of $f_{p,d}$ over $\Bbbk_p$, is a unique subfield of $\mathbb{K}$ with $[\Bbbk_{p,d} : \Bbbk_p] = d$.

□

Alright now let's do the problem. I just wanted to prove this all myself instead of looking over the notes. For now on I will refer to any finite field $\mathbb{K}$ as $\mathbb{F}_{p^n}$.

Problem 61. Let $\mathbb{K}$ be a finite field of characteristic $p > 0$.

(a) Prove that for every $n > 0$ there exists an irreducible polynomial $f \in \mathbb{K}[X]$ of degree n.

(b) Prove that for every irreducible polynomial $P \in \mathbb{K}[X]$ there exists $n \geq 0$ such that P divides $X^{p^n} - X$.

Proof. **(a)** We use the convention $\mathbb{K} = \mathbb{F}_{p^n}$ for some $n \in \mathbb{Z}^+$ since $\Bbbk$ is a finite field of characteristic p. By our theorems, there exists an extension $\mathbb{K}_m = \mathbb{F}_{p^{nm}}$ of degree m over $\mathbb{F}_{p^n}$. Suppose that for all $\alpha \in \mathbb{F}_{p^{nm}}$, the degree of α over $\mathbb{K}$ is strictly less than $[\mathbb{F}_{p^{nm}} : \mathbb{F}_{p^n}] = m$. So then by our theorems, any such α must belong to $\mathbb{F}_{p^n}(\alpha) \subset \mathbb{F}_{p^{nm}}$ and $[\mathbb{F}_{p^n}(\alpha) : \mathbb{F}_{p^n}] = d$ for some divisor $0 < d < nm$ of $[\mathbb{F}_{p^{nm}} : \Bbbk_n] = nm$. Once again, by our theorems, this must be the unique subfield $\mathbb{F}_{p^d}$ of order p^d. So then all elements of $\mathbb{F}_{p^{nm}}$ must belong to some unique proper subfield $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^{nm}}$ where $d \mid nm$.

Let $\{d_1, \ldots, d_k\}$ be the set of all divisors of nm that are less than nm, and let $d_{\max}$ be the maximal divisor of nm. By our theorems, we have the containment chain $\mathbb{F}_{p^{d_1}} \subset \mathbb{F}_{p^{d_2}} \subset \cdots \subset \mathbb{F}_{p^{d_{\max}}} \subset \mathbb{F}_{p^{nm}}$ and so in fact all elements of $\mathbb{F}_{p^{nm}}$ belong to $\mathbb{F}_{p^{d_{\max}}}$. But then $\mathbb{F}_{p^{d_{\max}}}$ isn't proper, a contradiction. Therefore, there exists an element $\alpha_m \in \mathbb{F}_{p^{nm}}$ with degree m over $\mathbb{F}_{p^n}$, and so there exists a monic irreducible polynomial of α_m over $\mathbb{F}_{p^n}$ with degree m, that is $\mathbb{F}_{p^{nm}} = \mathbb{F}_{p^{nm}}(\alpha_m)$. So for every $m > 0$ there exists an irreducible polynomial of degree m over $\mathbb{K} = \mathbb{F}_{p^n}$.

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

□

If the proper subset containment chain thing isn't allowed, I have another grosser proof with my original notation that makes a different argument on the next page.

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 $\langle 1 \rangle_+ = \Bbbk_p$-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 $f_{p,n,m} = x^{p^{nm}}$, respectively, over $\Bbbk_p$ 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 $[\mathbb{K}_m : \Bbbk_p] = nm$. Well, by our theorems this must be the unique subfield $\Bbbk_{p,d}$ of order p^d. Therefore,

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

a contradiction. (Another contradiction is just the fact that then every $\alpha \in \mathbb{K}_m$ belongs to $\Bbbk_{p,d}$ 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 $\Bbbk_p$. 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 $\Bbbk_p$, which is also a polynomial over $\mathbb{K}$.

□

Problem 62. 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 $n \geq 1$. 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 also have that d is smallest integer such that $\alpha^{p^{nd}} = \alpha$. Furthermore, $\alpha^{nk} = \alpha \iff d \mid k$.

($\implies$) If $f(x)$ is irreducible over $\mathbb{F}_{p^{nm}}$, then α has degree d over both $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^{nm}}$. So $\alpha = k_1 = k_2$ is the smallest integer such that $\alpha^{p^{nk_1}} = \alpha^{p^{nmk_2}} = \alpha$. Additionally, the previous equalities hold for any multiples $k_1, k_2 \geq 1$ of d. Suppose $g = \gcd(d,m) > 1$, then $\frac{d}{g} = \ell_d < d$, $\frac{m}{g} = \ell_m < m$. Observe.

$$m\ell_d = m\frac{d}{g} = \frac{m}{g}d = d\ell_m \implies \alpha^{p^{nm\ell_d}} = \alpha^{p^{nm(\frac{d}{g})}} = \alpha^{p^{nd(\frac{m}{g})}} = \alpha^{p^{nd\ell_m}} = \alpha.$$

But then there is a smaller positive integer $k_2 = \ell_d < d$ such that $\alpha^{nmk_2} = \alpha$, a contradiction. So we must have that $\gcd(d,m) = 1$.

($\impliedby$) On the other hand, if $\gcd(d,m) = 1$, recall that that d is the smallest positive integer $d = k_1$ such that $\alpha^{p^{nk_1}} = \alpha$ for any zero α of $f(x)$. So for any $k_2 \geq 1$ such that $\alpha^{p^{nmk_2}} = \alpha$, we must have that $d \mid mk_2$. Suppose we have such a k_2 less than d. But then $\gcd(d,m) = 1$ and $d \mid mk_2 \implies d \mid k_2$ and $k_2 < d$, which is impossible. So the smallest such $k_2 = d$, which is also the degree of α over $\mathbb{F}_{p^{nm}}$. Since degree of any zero α of $f(x)$ is d over $\mathbb{F}_{p^{nm}}$, $f(x)$ must be irreducible over $\mathbb{F}_{p^{nm}}$. (Otherwise we have some minimal polynomial of degree less than d which can be pulled out of $f(x)$ over $\mathbb{F}_{p^{nm}}$).

□

Problem 63. 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?

Proof. Let $p(x) = x^4+x^3+1 \in \mathbb{F}_2$. $p(0) = p(1) = 1 \neq 0$, so $P(x)$ has no zeros in $\mathbb{F}_2$ and therefore no linear factors over $\mathbb{F}_2$, and so it can't factor into a linear and cubic. Suppose $P(x)$ is reducible. Then must split into two irreducible quadratics over $\mathbb{F}_2$. Well, $x^2+1 = (x+1)(x-1)$ and $x^2+x = x(x+1)$, and $x^2 = x(x)$ over $\mathbb{F}_2$. Since x^2+x+1 is the only irreducible quadratic over $\mathbb{F}_2$, we must have that $P(x) = (x^2+x+1)^2$. Recall that Char $\mathbb{F}_2 = 2$ and so $(f(x)+g(x))^2 = (f(x))^2+(g(x))^2$ over $\mathbb{F}_2$. But then

$$P(x) = x^4+x^3+1 = ((x^2)+(x+1))^2 = x^4+(x+1)^2 = x^4+x^2+1, \text{ a contradiction.}$$

So then $P(x) = x^4+x^3+1$ is irreducible of degree 4 over $\mathbb{F}_2$ and for any zero α of $P(x)$

$$\mathbb{F}_2[x]/\langle x^4+x^3+1\rangle = \text{Span}_{\mathbb{F}_2}\{[1],[x],[x^2],[x^3]\} \cong \text{Span}_{\mathbb{F}_2}\{1,\alpha,\alpha^2,\alpha^3\} = \mathbb{F}_2(\alpha).$$

So $\mathbb{E} = \mathbb{F}_2[x]/\langle x^4+x^3+1\rangle$ is a 4-dimensional $\mathbb{F}_2$-vector space and we must have that $|\mathbb{E}| = 2^4 = 16$. For the remainder of this proof we will exclusively work in $\mathbb{E}$ and so we refer to cosets $[f(x)]_{\mathbb{E}}$ by any of their representatives $f(x)$ and let modulo x^4+x^3+1 be implied.

So $\mathbb{E} = \text{Span}\{1,x,x^2,x^3\}$ and since $x^4+x^3+1 = 0$ in this field, $x^4 = -x^3-1 = x^3+1$, and obviously x is a root of $p(x) = x^4+x^3+1$ over $\mathbb{E}$. Then, recall that since $\mathbb{E} \cong \mathbb{F}_{2^4}$, is a finite field extension of $\mathbb{F}_2$ with characteristic 2, we must have that the Frobenius mapping $\varphi_2 \coloneqq x \mapsto x^2$ is an endomorphism of $\mathbb{E}$ (In fact it is a isomorphism in $\text{Aut}_{\mathbb{F}_2}(\mathbb{F}_{2^4})$) and so it permutes roots of polynomials in $\mathbb{E}[x]$ to each other. Well, $x^4 = x^3+1 \implies x^5 = x(x^4) = x(x^3+1) = x^4+x = x^3+x+1 \implies x^6 = x(x^5) = x(x^3+x+1) = x^4+x^2+x = (x^3+1)+x^2+x = x^3+x^2+x+1$.

Therefore, the orbit $\text{Orb}_{\varphi_2}(\mathbb{E}) = \{x\} \cup \{x^2\} \cup \{x^4 = x^3+1\} \cup \{x^8 = (x^4)^2 = (x^3+1)^2 = x^6+1 = (x^3+x^2+x+1)+1 = x^3+x^2+x\} \cup \cdots = \{x,x^2,x^3+1,x^3+x^2+x\}$ must be all roots of $P(x) = x^4+x^3+1$ over $\mathbb{E}$, since they are four distinct elements and $P(x)$ has at most four distinct roots.

□

Problem 64. Prove that an algebraic extension of a perfect field is a perfect field.

Proof. Let $\mathbb{K}$ be a perfect field. If $\mathbb{K}$ has characteristic 0, then so does any extension of it since they share 1, and so any algebraic extension of $\mathbb{K}$ must be perfect.

If $\mathbb{K}$ has characteristic $p > 0$. Since $\mathbb{K}$ is perfect, every irreducible polynomial $f(x)$ over $\mathbb{K}$ has no repeated roots in some splitting field $\mathbb{F}_{f(x)}$ of $f(x)$. That is, the minimal polynomial of any algebraic element has no repeated linear factors in $\mathbb{F}_{P(x)}$.

Therefore, if $\mathbb{E}$ is some algebraic extension of $\mathbb{K}$, then any $\alpha \in \mathbb{E}$ is algebraic over $\mathbb{K}$. It's minimal polynomial $P_{\alpha,\mathbb{K}}(x)$ over $\mathbb{K}$ has no repeated roots some splitting field $\mathbb{F}_{P(x)}$ of $P(x)$. Now, since α is a zero of $P_{\alpha,\mathbb{K}}(x)$ which also belongs to $\mathbb{E}[x]$, the minimal polynomial $P_{\alpha,\mathbb{E}}(x)$ of α over $\mathbb{E}$ must divide $P_{\alpha,\mathbb{K}}(x)$ over $\mathbb{E}$. Therefore, $P_{\alpha,\mathbb{E}}(x)$ must split completely over $\mathbb{F}_{P(x)}$ into distinct linear factors as well, since otherwise $P_{\alpha,\mathbb{K}}(x)$ is divisible by some repeated linear factor of $P_{\alpha,\mathbb{E}}(x) \mid P_{\alpha,\mathbb{K}}(x) \in \mathbb{F}_{P(x)}[x]$, a contradiction. So every minimal polynomial over $\mathbb{E}$ is seperable. Since every irreducible polynomial over $\mathbb{E}$ is simply some minimal polynomial of one of it's zeros, which we proved is seperable, scaled by some $c \in \mathbb{E}$, every irreducible over $\mathbb{E}$ is also seperable. Therefore, $\mathbb{E}$ is perfect.

□

Problem 65. Show that the extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt[4]{2}, i\right)$ is Galois. Find its Galois group.

Proof. $\sqrt[4]{2}$ and i have minimal polynomials x^4-2 and x^2+1 over $\mathbb{Q}$ they are both algebraic over $\mathbb{Q}$ and so $\mathbb{Q}(\sqrt[4]{2}, i)$ is a finite, and therefore algebraic extension of $\mathbb{Q}$. Since $\mathbb{Q}$ has characteristic 0, it is perfect, and so is any algebraic extension of it such as $\mathbb{Q}(\sqrt[4]{2}, i)$. So then $\mathbb{Q}(\sqrt[4]{2}, i)$ is seperable.

Now, notice that $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$ are all zeros of x^4-2. Well, x^4-2 has at most 4 distinct zeros over $\mathbb{C}$, and so these must be all of them. Well, any extension $\mathbb{E}$ where x^4-2 splits completely over must contain i and $\sqrt[4]{2}$, so $\mathbb{Q}(\sqrt[4]{2}, i) \subseteq \mathbb{E}$. Therefore, $\mathbb{Q}(\sqrt[4]{2}, i)$ must be a splitting field for x^4-2. Therefore, since $\mathbb{Q}(\sqrt[4]{2}, i)$ is a splitting field of some polynomial over $\mathbb{Q}$, it is normal. Finally, since $\mathbb{Q}(\sqrt[4]{2}, i)$ is seperable and normal, it must be Galois. Now, since x^4-2 is monic and irreducible over $\mathbb{Q}(i)$, $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] = 4$ and $|\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})| = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 8$.

Let $a = \sqrt[4]{2}$ and $b = i$. So the conjugates of a are $\{a, -a, ba, -ba\}$ and the conjugates of b are $\{b, -b\}$. Also recall that that $a^4 = (\sqrt[4]{2})^4 = 2$ and $b^2 = i^2 = -1$. Now, we denote automorphisms in $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(a,b)/\mathbb{Q})$ that sends an adjoined root $\alpha \in \{a, b\}$ to one of its conjugates α' and fixes the other adjoined root via $\phi_{\alpha,\alpha'} \coloneqq \alpha \mapsto \alpha$. Observe.

$$\phi_{b,-b}^2 \coloneqq \phi_{b,-b}(\phi_{b,-b}(b)) = \phi_{b,-b}(-b) = b \implies \phi_{b,-b}^2 = \mathrm{id}.$$

$$(\phi_{b,-b} \circ \phi_{a,ba})(a) = \phi_{b,-b}(ba) = -ba \neq ba = \phi_{a,ba}(a) = (\phi_{a,ba} \circ \phi_{b,-b})(a)$$

$$\implies \phi_{b,-b} \circ \phi_{a,ba} \neq \phi_{a,ba} \circ \phi_{b,-b}$$

Therefore, $\mathrm{Gal}(\mathbb{Q}(a,b)/\mathbb{Q})$ is a non-abelian group of order 8 with an element $\phi_{b,-b}$ of order 2. So then since it could only be isomorphic to Q_8 or D_4 purely by order, and Q_8 has no elements of order 2, we must have that $\mathrm{Gal}(\mathbb{Q}(a,b)/\mathbb{Q}) \cong D_4$.

□