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 $1 = [\mathbb{K}(a):\mathbb{K}] = [\mathbb{F}:\mathbb{K}] \mid 1!$. If f has degree 2 over $\mathbb{K}$, then it has at most two distinct zeros. Suppose f is redicible. 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 $x^2-(a_1+a_2)x+a_1a_2 = x^2+bx+c \implies a_2 = -b-a_1 \in \mathbb{K}(a)$ 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,

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

$\square$

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 $\mathrm{Aut}_{\mathbb{Q}}\big(\mathbb{Q}(\sqrt{d})\big)$ 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 $\mathbb{Q}$?

Problem 60. Assume K is a field of characteristic 0. Let G be the subgroup of $\mathrm{Aut}_K\big(K(X)\big)$ 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 $[K(X):E]$?

Problem 61. 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 $X^{p^n} - X$.

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.

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?

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

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