Problem 1. Let $G$ be a finite simple group which contains an element of order 55. Prove that the index of any proper subgroup of $G$ is at least 16.

Solution. Let $H \subset G$ be a proper subgroup of index $n = [G : H]$. The action of $G$ on the set of left cosets $G/H$ defines a homomorphism $\rho: G \to S_n$ to the symmetric group on $n$ elements. The kernel $\ker(\rho)$ is a normal subgroup of $G$ which is contained in the proper subgroup $H$, so $\ker(\rho)$ must be trivial as $G$ is simple. Thus, $\rho$ is injective and $S_n$ contains an element $\sigma$ of order 55. The order of an element of $S_n$ is the least common multiple of the lengths of the cycles in its cycle decomposition, so $\sigma$ must decompose into a product of disjoint cycles of lengths 5 and 11. In particular, $n \geq 5 + 11 = 16$.

Problem 2. Prove that any group of order 455 = 5 · 7 · 13 is abelian.

Solution. The Sylow theorems show there exists either 1 or 91 Sylow 5-subgroups, there is a unique Sylow 7-subgroup $N_7 \subset G$, and there is a unique Sylow 13-subgroup $N_{13} \subset G$, with $N_7$ and $N_{13}$ both normal. The map $G \to G/N_7 \times G/N_{13}$ is injective since $N_7$ and $N_{13}$ have relatively prime orders. We win since $G/N_7$ and $G/N_{13}$ are abelian by the following observation: For primes $p < q$ with $q \not\equiv 1 \pmod{p}$, any group $A$ of order $pq$ splits as a product $A \cong \mathbb{Z}/p \times \mathbb{Z}/q$. (Indeed, by the Sylow theorems there are normal subgroups $P \subset A$ and $Q \subset A$ of sizes $p$ and $q$, and for order reasons we must have $P \cap Q = \{1\}$ and $PQ = A$, hence $A \cong P \times Q$ splits as the direct product.)

Problem 3. Let $f(x) \in k[x]$ be an irreducible polynomial where $k$ is a field of characteristic 0 with algebraic closure $\bar{k}$. Prove that there does not exist an element $a \in \bar{k}$ so that $f(a) = f(a+1) = 0$.

Solution. Let $K \subset \bar{k}$ be the splitting field for $f(x)$ in $\bar{k}$. Since $f(x)$ is irreducible, the Galois group $\text{Gal}(K/k)$ acts transitively on the roots of $f(x)$. In particular, if $a \in \bar{k}$ is such that $f(a) = f(a+1) = 0$, then $a \in K$ and there exists $\sigma \in \text{Gal}(K/k)$ such that $\sigma(a) = a + 1$. Then $\sigma^n(a) = a + n$ is a root of $f(x)$ for every integer $n$. Since the number of roots of $f(x)$ is finite, this is only possible if the characteristic of $k$ is positive.

Problem 4. Let $f(x) \in F[x]$ an irreducible, separable polynomial over a field $F$, and let $E$ be a splitting field for $f(x)$ over $F$. Prove that if $\text{Gal}(E/F)$ is abelian, then for any root $a \in E$ of $f(x)$ we have $E = F(a)$.

Solution. Since $\text{Gal}(E/F)$ is abelian any subgroup is normal, so by the Galois correspondence $K/F$ is Galois for any intermediate field extension $F \subset K \subset E$. In particular, for any root $a$ of $f(x)$ the extension $F(a)/F$ is Galois, so it must contain every root of the polynomial $f(x)$, i.e. $F(a) = E$.

Problem 5. Prove that $Q(\sqrt{2} + \sqrt{2})$ is a Galois field extension of $Q$, and compute its Galois group.

Hint: The following two facts may be useful.
(1) (Eisenstein’s criterion) If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and $p$ is a prime such that $p$ divides all $a_i$ but $p^2$ does not divide $a_0$, then $f(x)$ is irreducible as an element of $\mathbb{Q}[x]$.

(2) If $\alpha = \sqrt{2} + \sqrt{2}$ and $\beta = \sqrt{2} - \sqrt{2}$, then $\alpha \beta = \sqrt{2}$

Solution. A computation shows that $f(x) = x^4 - 4x^2 + 2$ has roots $\pm \alpha$ and $\pm \beta$, where $\alpha = \sqrt{2} + \sqrt{2}$ and $\beta = \sqrt{2} - \sqrt{2}$. We claim $K = \mathbb{Q}(\sqrt{2} + \sqrt{2})$ is the splitting field of $f(x) = x^4 - 4x^2 + 2$, and hence is Galois. Clearly $\pm \alpha \in K$. Note that $\sqrt{2} = \alpha^2 - 2 \in K$, so from $\alpha \beta = \sqrt{2}$ we find $\pm \beta \in K$ as well.

Next we prove that $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4$. First note that the polynomial $f(x) \in \mathbb{Q}[x]$ is irreducible by Eisenstein’s criterion at the prime 2. Thus $[K : \mathbb{Q}] = 4$ and we have either $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4$ or $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. To show the first case holds, it suffices to show that there exists $\sigma \in \text{Gal}(K/\mathbb{Q})$ of order greater than 2. Choose $\sigma$ so that $\sigma(\alpha) = \beta$. From the computations above we find $\beta = (\alpha^2 - 2)/\alpha$, and thus

$$\sigma^2(\alpha) = \frac{\beta^2 - 2}{\beta} = -\frac{\sqrt{2}}{\sqrt{2} - \sqrt{2}} = -\frac{\sqrt{2}}{\beta} = -\alpha.$$ 

This shows $\sigma$ has order greater than 2.