Problem 1. Let $p$ be a prime number. Let $G$ be a group of order $p^k$ for $k \geq 1$ and let $H$ be the subgroup of $G$ generated by elements of the form $g^p$. Show that $H \neq G$.

Solution: A $p$-group is always nilpotent and thus has a nontrivial abelian quotient. Let $\alpha : G \to A$ be a quotient map with $A$ a nontrivial abelian $p$-group. A nontrivial abelian $p$-group always has a quotient map onto $\mathbb{Z}/p\mathbb{Z}$ so, composing with this quotient, we get a surjection $\beta : G \to \mathbb{Z}/p\mathbb{Z}$. Then every $g^p$ lies in the kernel of $\beta$.

Problem 2. Let $K/F$ be a field extension of degree $n$. Show that there is a subgroup of $\text{GL}_n(F)$ which is isomorphic to $K^\times$.

Solution: Choose a basis $e_1, e_2, \ldots, e_n$ for $K$ over $F$. For each $\alpha$ in $K$, multiplication by $\alpha$ is an $F$-linear map form $K$ to $K$; writing this map in the basis $e_1, e_2, \ldots, e_n$ gives an $n \times n$ matrix $\rho(\alpha)$. We have $(\alpha \beta) \gamma = \alpha (\beta \gamma)$, showing that $\rho(\alpha \beta) = \rho(\alpha) \rho(\beta)$, so $\rho$ is a group homomorphism. The last detail to check is that this map is injective. Indeed, we always have $\rho(\alpha)(1) = \alpha \cdot 1 = \alpha$, so the only $\alpha$ with $\rho(\alpha) = \text{Id}$ is $\alpha = 1$.

Problem 3. Let $F$ be a field. $\text{GL}_n(F)$ is the group of invertible $n \times n$ matrices with entries in $F$ and $\text{SL}_n(F)$ is the subgroup of matrices of determinant 1. Prove or disprove: There is an action of $F^\times$ on $\text{SL}_n(F)$ such that $\text{GL}_n(F) \cong \text{SL}_n(F) \rtimes F^\times$.

Solution: The statement is true! Embed $F^\times$ into $\text{GL}_n(F)$ by sending $\alpha$ to the diagonal matrix with entries $(\alpha, 1, 1, \ldots, 1)$. This embedding is split by the determinant map $\det : \text{GL}_n(F) \to F^\times$. So $\text{GL}_n(F)$ is the semidirect product of $F^\times$ and the kernel of $\det$, namely $\text{SL}_n(F)$. Explicitly, the action of $\alpha \in F^\times$ on $\text{SL}_n(F)$ is conjugation by $\text{diag}(\alpha, 1, 1, \ldots, 1)$.

Problem 4. Let $K/Q$ be a Galois extension with degree 9 and at least 2 distinct subfields $Q \subseteq L_1, L_2 \subseteq K$. What is $\text{Gal}(K/Q)$?

Solution: The two groups of order 9 are $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. The group $\mathbb{Z}/9\mathbb{Z}$ only has one nontrivial proper subgroup so, by the Galois correspondence, $\text{Gal}(K/Q)$ must be $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

Problem 5. Let $\zeta$ be a primitive 7-th root of unity. Give an explicit element $\gamma$ of $Q(\zeta)$ such that $\gamma$ is not in $Q$ but $\gamma^2$ is in $Q$. You may assume that the cyclotomic polynomial $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ is irreducible.

Solution: We recall that the Galois group of $Q(\zeta)/Q$ is $(\mathbb{Z}/7\mathbb{Z})^\times$, where $a \in (\mathbb{Z}/7\mathbb{Z})^\times$ acts on $Q(\zeta)$ by $\zeta \mapsto \zeta^a$. (For the record, we recall the proof: Since $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, the Galois group must act transitively on the roots of this polynomial, which are $\{\zeta^a : a \in (\mathbb{Z}/7\mathbb{Z})^\times\}$. So, for each $a \in (\mathbb{Z}/7\mathbb{Z})^\times$, we must have some $\sigma_a$ in the Galois group with $\sigma_a(\zeta) = \zeta^a$. To check that the group structure is $(\mathbb{Z}/7\mathbb{Z})^\times$, note that $\sigma_a(\sigma_b(\zeta)) = \sigma_a(\zeta^b) = \sigma_a(\zeta)^b = (\zeta^a)^b = \zeta^{ab}$ where, in the penultimate equality, we have used that $\sigma_a$ respects the field multiplication.) We note that $(\mathbb{Z}/7\mathbb{Z})^\times$ has a homomorphism $\chi$ to $\{\pm 1\}$, with $\chi(1) = \chi(2) = \chi(4) = 1$ and $\chi(3) = \chi(5) = \chi(6) = -1$.

Set $\gamma = \sum_{a \in (\mathbb{Z}/7\mathbb{Z})^\times} \chi(a) \zeta^a$. Then, for $b \in (\mathbb{Z}/7\mathbb{Z})^\times$, we have $\sigma_b(\gamma) = \chi(b) \gamma$. In particular, $\sigma_3(\gamma) = \sigma_5(\gamma) = \sigma_6(\gamma) = -\gamma$ so $\gamma$ is not fixed by the Galois group, and hence is not rational. (Since $\sigma_6$ is complex conjugation, $\gamma$ isn’t even real!) But $\gamma^2$ is fixed by every $\sigma_b$, so $\gamma^2$ is rational. In fact, one can compute that $\gamma^2 = -7$. 