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 β.

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

Solution: Choose a basis e_1, e_2, …, e_n for K over F. For each α in K, multiplication by α is an F-linear map form K to K; writing this map in the basis e_1, e_2, …, 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 ρ 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 α with $\rho(\alpha) = \mathrm{Id}$ is $\alpha = 1$.

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

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

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

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, $\mathrm{Gal}(K/\mathbb{Q})$ must be $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

Problem 5. *Let ζ be a primitive 7-th root of unity. Give an explicit element γ of $\mathbb{Q}(\zeta)$ such that γ is not in $\mathbb{Q}$ but γ^2 is in $\mathbb{Q}$. 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 $\mathbb{Q}(\zeta)/\mathbb{Q}$ is $(\mathbb{Z}/7\mathbb{Z})^\times$, where $a \in (\mathbb{Z}/7\mathbb{Z})^\times$ acts on $\mathbb{Q}(\zeta)$ 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 σ_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 σ_a respects the field multiplication.) We note that $(\mathbb{Z}/7\mathbb{Z})^\times$ has a homomorphism χ 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 γ is not fixed by the Galois group, and hence is not rational. (Since σ_6 is complex conjugation, γ isn't even real!) But γ^2 is fixed by every σ_b, so γ^2 is rational. In fact, one can compute that $\gamma^2 = -7$.