**Math 250A CRN: 38753, Final Thursday, Dec 8 Fall 2022**

Name:

1. (Frobenius)
   Assume that $p$ and $r$ are primes and write $q = p^r$, $\phi \in Aut\mathbb{F}_q$ for the Frobenius automorphism (defined by $\phi(a) = a^p$) and $C \leq Aut\mathbb{F}_q$ for the cyclic group generted by $\phi$.
   Show that all the orbits of the action of $C$ on $\mathbb{F}_q - \mathbb{F}_p$ are the same size.
   Hint: Show that there are no intermediate fields.

2. (Sylow)
   Show that no group of order 30 is simple.
   Hint: Show that if $G$ is a finite simple group and $n_p$ is the number of $p$-Sylow subgroups of $G$ for some $p$ dividing $|G|$ then $|G|$ divides $n_p!$.

3. (Splitting)
   Consider the complex number $a = \sqrt{6} + \sqrt{10} + \sqrt{15}$.
   Take $p(x) \in \mathbb{Q}[x]$ to be the minimal polynomial for $a$ over $\mathbb{Q}$.
   Take $K = Spl_{\mathbb{Q}}(p)$ to be the splitting field.
   Find the Galois group $Aut(K)$.
   Hints: There is no need to find the minimal polynomial.
   Show that $K$ is a **proper** subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

4. (Algebraic)
   Assume that $\alpha, \beta \in \mathbb{C}$ are complex numbers and $p(x) = \sum_{i=0}^{n} a_i x^i$, $q(x) = \sum_{i=0}^{m} b_i x^i \in \mathbb{C}[x]$ are polynomials with $p(\alpha) = q(\beta) = 0$.
   Write $K = \langle a_0, \ldots a_n, b_0, \ldots b_m \rangle \subseteq \mathbb{C}$ for the subfield of $\mathbb{C}$ generated by the coefficients of $p$ and $q$.
   Show that there is another polynomial $r(x) \in K[x]$ with $r(a + b) = 0$.

5. (Semidirect)
   Show that if $G = A \rtimes_{\phi} (B \rtimes_{\psi} C)$ then there are $N$ and $\rho$ so that $G = N \rtimes_{\rho} C$.

6. (Separability)
   Find the number of (distinct) roots of $p(x) = x^6 + yx^3 + y \in \overline{\mathbb{F}_3(y)}[x]$.

7. (Isomorphisms)
   If $Y \leq H$ is a subgroup and $f : X \to H$ is a group homomorphism with image contained in the normalizer of $Y$ then
   $$[Im(f) \cdot Y]/Y \cong X/f^{-1}(Y).$$
   Note: This makes a nice braid-like commutative diagram.