Instructions: The exam contains seven questions, and you should hand in answers to all seven of them.

You may freely use any notes or statements from class or the textbook. It is also permissible to use outside sources, or to talk with me about the exam questions, but if you do this be sure to acknowledge these discussions or references in your write up of those questions. You should, of course, try and do as much on your own as possible.

The exam is due on or before **Wednesday, April 13, 2016**, by **23:59:59**.

1. [Medium answer] Suppose that $K \subseteq L$ is an extension of fields of finite degree.

   (a) Explain the inductive argument showing that $|\mathrm{Aut}(L/K)| \leqslant [L : K]$. In the case that $|\mathrm{Aut}(L/K)| = [L : K]$ explain how the inductive step shows that $K \subseteq L$ is a separable normal extension.

   (b) Conversely, assume that $K \subseteq L$ is a separable normal extension. Explain how we know that $|\,\mathrm{Aut}(L/K)| = [L : K]$. You may use the lifting lemma and facts about normal and separable extensions without proof, but be sure to mention how you're using them. (That is, in this question, I would like you to give a 'bird's eye view' of the argument. You don't have to provide all the proofs of the various lemmas and propositions we used, but do explain how all the pieces fit together to get this result.)

2. [Short answer] Suppose that K is a field, and that $f(x) = x^3 + bx^2 + cx + d \in K[x]$ is a cubic polynomial with roots α_1, α_2, and α_3 (Note: the roots might not be in K).

   (a) Explain why the sum $\alpha_1^5 + \alpha_2^5 + \alpha_3^5$ can be computed as a polynomial in b,c, and d, without ever having to find α_1, α_2, or α_3.

   (b) Find this polynomial. (Note: If you want to check your formula, the easiest way to do this is to choose roots α_1, α_2, and α_3, write out the cubic polynomial with those roots, then apply your formula to see if you get the answer you expect.)

3. [Very short answer] Suppose that K is a field of characteristic zero, and that $f(x) \in K[x]$ is an irreducible polynomial over K, with splitting field L.

   (a) If $\deg(f(x)) = 3$ what are the possibilities for the Galois group $G = \mathrm{Gal}(L/K)$? How can you distinguish between them?

   (b) If $\deg(f(x)) = 4$ what are the possibilities for the Galois group $G = \mathrm{Gal}(L/K)$? How do you decide between them?

4. [Long answer] Let $K = \mathbb{Q}(i)$, and let $f(x) \in K[x]$ be the polynomial $f(x) = x^4 + 0x^3 + 3x^2 + 0x - 1$; $f(x)$ is irreducible over K, a fact that you may assume without proof. Let L be the splitting field of f over K. Find all the roots of $f(x)$, find the Galois group $G = \mathrm{Gal}(L/K)$, and describe all the intermediate fields M, $K \subseteq M \subseteq L$ along with their inclusions.

This problem will likely take some organization, so please put some thought into what your notation will be, and in laying out your argument in a clean way.

One thing to note is that, if r is a positive real number, then the symbol $\sqrt{r}$ (or even $\sqrt[n]{r}$) has unambiguous meaning: it is the unique positive real number which is the square (or n-th) root of r. If c is a complex number, then the meaning of $\sqrt{c}$ is not so clear: there are two possibilities and no canonical way to distinguish between them. If you use a symbol like $\sqrt{c}$, be sure and indicate (perhaps by drawing a picture of the complex plane, or by specifying the "angle" of the root) which square root you mean. Any further time you use the symbol $\sqrt{c}$ I'll assume that you mean the same root, and that $-\sqrt{c}$ means the opposite root. Of course, if you have another complex number c' and want to write $\sqrt{c'}$, you'll have to go through the process all over again (similarly for $\sqrt[n]{c}$).

5. [Short answer and follow up question]: Let $f(x)$, K, and G be as in question 4, and L' the splitting field of $f(x)$ over $\mathbb{Q}$. What is the relation of the Galois group G from question 4 and the Galois group $G' = \mathrm{Gal}(L'/\mathbb{Q})$? What is the field L'? What is the group G'? Only short answers are required here, but you should mention your justifications for your statements.

6. [Short Answer] Let p be a prime, and $d \geqslant 2$. Explain how we know that $\mathbb{F}_{p^d}/\mathbb{F}_p$ is a Galois extension, and how we know that the group $\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p)$ is cyclic.

7. [Medium answer] Let $f(x) \in \mathbb{Q}[x]$ be the polynomial $x^{17} - 5$, and L the splitting field for $f(x)$ over $\mathbb{Q}$. Determine as much as you can about the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$. For instance, you should definitely find the order of G. Is G solvable? Can you say anything about the structure of G? (For instance, is it a product group? A semi-direct product?) Can you describe the p-Sylow subgroups of G? Can you describe all subgroups of G? How many are there of each order? (Note: You *do not have to*, and *should not* give all the intermediate fields corresponding to the subgroups of G, nor do you need to figure out the lattice of subgroups of G.) All claims should be justified, and the clarity of your explanation is important.

Some Formulae

- A cubic $x^3 + bx^2 + cx + d$ has discriminant $b^2c^2 + 18bcd - 4b^3d - 4c^3 - 27d^2$.
- A quartic $x^4 + bx^3 + cx^2 + dx + e$ has resolvent cubic

$$p(t) = t^3 - ct^2 + (bd - 4e)t + (4ce - d^2 - b^2e).$$

- To compute the discriminant of a quartic, first compute its resolvent cubic, and then the discriminant of that cubic. This will be the same as the discriminant of the quartic computed directly.