The second exam will cover all the material we have discussed since the first exam. This means basically groups, although recall we have also discussed how groups relate to fields and polynomials, and to counting problems. Note that while field extensions was covered on the previous exam, you should be familiar enough with that material to answer questions about the relationship between groups and field (Galois Theory). So in that sense, this is really a cumulative exam. Here is a checklist of these topics.

- ☐ Working in S_n
  - ◯ Cayley's Theorem (groups isomorphic to subgroups of S_n).
  - ◯ Notation: disjoint cycles; transpositions
  - ◯ Even and odd permutations.
  - ◯ Orders of elements and their relationship to Galois groups
- ☐ Subnormal series, composition series, solvable groups.
- ☐ Galois correspondence.
- ☐ Solvability by radicals.
- ☐ The order of elements in general (don't forget the division algorithm).
- ☐ Cyclic groups and the relationship to order.
- ☐ Fermat's Little and Euler's Theorem, and their relationship to RSA cryptography; Euler's φ-function.
- ☐ p-groups; inner direct products;
- ☐ The Fundamental Theorem of Finite Abelian Groups.
- ☐ Group actions, stabilizers, fixed point sets, and orbits.
- ☐ The orbit-stabilizer theorem.
- ☐ Burnside's counting theorem.

The homework and class activities should give you a good idea of the types of questions to expect. Additionally, the questions below would all make fine exam questions.

Sample Questions

1. The group D_3 of symmetries of the triangle is isomorphic to S_3. But by Cayley's theorem, the group is also isomorphic to a *subgroup* of S_6. Find such a subgroup (using the proof of Cayley's theorem).

2. The identity can be written as $\varepsilon = (13)(24)(35)(14)(12)(15)(34)(45)$. Mimic the proof that ε must be even and show how to eliminate $x = 5$ from the product of transpositions and write ε as the product of 2 fewer transpositions in the process. Show all intermediate steps.

3. Suppose the group G has subnormal series

$$G \supset H \supset \{e\}$$

and that $G/H \cong \mathbb{Z}_{10}$. Assume also that H is simple.

   (a) Explain how we know that the above series is not a composition series.

   (b) Explain how we could find two different composition series for G.

   (c) Prove that if H is abelian, then G is solvable.

   (d) If G happens to be the Galois group for some field E over $\mathbb{Q}$, what can you say about subfields of E?

4. Consider the polynomial $p(x) = x^3 + 5x^2 - 10x + 15$. Let E be the splitting field for $p(x)$ and G be the Galois group of E over $\mathbb{Q}$.

   (a) Prove that G contains an element of order 3.

   (b) Prove that G contains an element of order 2.

   (c) Explain how we know that there is a intermediate field I strictly between $\mathbb{Q}$ and E that is the splitting field for a polynomial. What can you say about this field?

   (d) Explain how you know that $G \cong S_3$ and not to $\mathbb{Z}_6$.

   (e) Does the argument above prove that $p(x)$ is not solvable by radicals? Is $p(x)$ solvable by radicals?

5. Consider the number $n = 1643 = 31 \cdot 53$.

   (a) What is 42^{1560} congruent to modulo 1643? Explain, using group theory. What if we replaced 42 with another number?

   (b) Note that $E = 7$ is relatively prime to 1643. Find an integer D such that $(a^7)^D \equiv a \pmod{1643}$ for any a relatively prime to 1643. Explain how you know your D works.

6. What is the difference between an inner direct product and an external direct product? Illustrate with an example.

7. I'm thinking of an abelian group that contains elements of order 9 but not of order 27, and elements of order 2 and 5 but not of orders 4 or 25. Further, there is not other prime number p (other than 2, 3, or 5) such that there is an element of order p. Which of the following can you deduce about my group? Which must be true, which can't be true, and which might or might not be true.

   (a) There are elements of order 3.

   (b) There are elements of order 10.

   (c) The group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$.

   (d) The group is cyclic.

8. Find all abelian groups of order 480.

9. Let $X = \{1, 2, 3, 4, 5, 6\}$ and $G = \{(1), (12), (345), (354), (12)(345), (12)(354)\}$. Find X_g, G_x and $\mathcal{O}_x$ for each $g \in G$ and $x \in X$. Then verify the orbit-stabilizer theorem and Burnside's theorem.

10. How many different ways could the vertices of an equilateral triangle be colored using three colors?

11. Use Burnside's theorem to explain why $\binom{7}{3} = \frac{1}{3!}P(7,3)$. That is, why are there 6 times as many ways to make three scoop ice-cream cones chosen from 7 flavors as there are to make three scoop milkshakes (cones and shakes not allowing for repeated flavors).