Math 322 **Exam 2 Study Guide** Spring 2019

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. 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.

- □ Cayley's Theorem (groups isomorphic to subgroups of S_n).
- □ Working in S_n
  - ○ Cycle notation.
  - ○ Products, powers, inverses, etc.
  - ○ Writing permutations as products of disjoint cycles.
  - ○ Even and odd permutations; transpositions.
  - ○ Orders of permutations
- □ The order of elements (don't forget the division algorithm).
- □ Cyclic groups and the relationship to order.
- □ The theorems of Lagrange and Cauchy.
- □ Fermat's Little and Euler's Theorem, and their relationship to RSA cryptography.
- □ p-groups.
- □ The Fundamental Theorem of Finite Abelian Groups.
- □ Subnormal series, composition series, solvable groups.
- □ Galois correspondence.
- □ Solvability by radicals

The homework and class activities should give you a good idea of the types of questions to expect. Also take a look at the quizzes we did over this material. Copies of these assignments, with solutions, are available on Canvas.

Additionally, the questions below would all make fine exam questions.[1]

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. Consider the following permutations in S_5

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$$

[1] Disclaimer: Question on the actual exam may be easier or harder than those given her. There might be types of questions on this study guide not covered on the exam and questions on the exam not covered in this study guide. Questions on the exam might be asked in a different way than here. If solving a question lasts longer than four hours, contact your professor immediately.

(a) Find fg.

(b) Find f^{-1}

(c) Find fgf^{-1}

(d) Find $f^3g^2fg^{-1}$

(e) Write f and g as cycles or the product of disjoint cycles.

(f) Write f and g as products transpositions

(g) Write all the answers to parts (a)-(d) both as cycles or the product of disjoint cycles and as the product of transpositions

4. Consider the group S_5, which has 120 elements.

   (a) If $\alpha \in S_5$, find α^{120}. Explain.

   (b) Is there an element of order 120? Explain.

   (c) Is there an element of order 6? Explain.

   (d) Is there an element of order 7? Explain.

5. Let G be a group with elements a and b.

   (a) True or false: $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$? Explain why or give a counterexample.

   (b) True or false: $\operatorname{ord}(ab) = \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$? Explain why or give a counterexample.

   (c) True or false: $\operatorname{ord}(ab) | \operatorname{ord}(a)\operatorname{ord}(b)$? Explain why or give a counterexample.

   (d) For any of the three statements above which are false, are they true if a and b commute? What else would you need to assume to make the statements true?

6. Let G be a cyclic group generated by a and let H be a subgroup of G. Prove that G/H is cyclic.

7. Suppose $G = \langle a \rangle$ is cyclic with order n.

   (a) What must be true of any subgroup H of G?

   (b) Prove that for every k which divides n, there is a subgroup of order k.

   (c) Is part (b) necessarily true if G is not cyclic? Hint: look at the subgroups of A_4.

8. Consider the group $\mathbb{Z}_{17}$. Find all subgroups and justify your answer.

9. State Lagrange's theorem and explain what it means. Briefly explain how we know it is true (do not give a full proof – just explain the key steps).

10. State Cauchy's theorem and explain what it means. Briefly explain how we proved Cauchy's theorem for abelian groups (do not give the full proof – just explain the key steps).

11. Find all abelian groups of order 480.

12. 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?

13. 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?