Algebraic Structures Homework #5
Due Monday, December 8

The final homework assignment is an in class presentation. You will each have 20 minutes to present a topic selected from one of the following options.

1. **Public Key Cryptography**

   (a) Describe the idea behind public-key cryptography and explain how it is different than private-key cryptography.

   (b) Describe the RSA algorithm for public-key cryptography. (Joseph Gallian's textbook *Contemporary Abstract Algebra* has an excellent introduction to RSA in chapter 8. There are also good descriptions online.)

   (c) Make sure you explain why the algorithm works.

2. **Ruler and Compass Constructions**

   (a) What is a ruler and compass construction?

   (b) Show how to use a ruler and compass to find the midpoint of a line segment, to find the bisector of a angle, and to construct an equilateral triangle.

   (c) Are there any regular polygons that can't be constructed using a ruler and compass?

   (d) Read Section 32 in the textbook. Describe the constructible numbers and explain in words why they form a field.

   (e) Conclude your paper by describing two impossible constructions (in addition to the impossible construction in part (c)).

3. **Extension Fields and Transcendental Numbers**

   (a) Read the beginning of Section 29 in the textbook. Define an extension field and state Kronecker's Theorem. How is Kronecker's theorem related to the Fundamental Theorem of Algebra?

   (b) Define the terms *algebraic number* and a *transcendental number.*

   (c) One proof that transcendental numbers exist uses a counting argument. Sketch this proof by answering the following questions.

      i. How many real numbers are there?

      ii. How many polynomials with integer coefficients are there?

      iii. How many algebraic numbers are there?

   (d) Give three examples of transcendental numbers, and for each example find out when the example was proven to be transcendental.

   (e) Try to give a timeline for the major exents you have talked about. Tell us who proved each result and when they did it.