Here is the plan for the rest of the semester. We will spend the next two weeks or so (up to Spring Break) exploring some of the structure of groups, enough to understand Galois groups and prove that there are polynomials whose roots cannot be expressed using radicals. In the 6 weeks after Spring Break, we will explore some additional topics in abstract algebra.

The choice of which topics is largely up to you. There are lots of interesting things we can explore, way more than we have time for. So some topics will be tackled as a class, while others will be the basis for your group final projects. More on the structure of the final project below.

Here are some topics that I think would be interesting. I've tried to provide a very short description of each, but feel free to look them up on Wikipedia to get a better idea of what they are about. I'd like you to rank these (a survey will be available on Canvas) and identify any that you would particularly like to do either as a class or as your project. If there is another topic you are interested in, please let me know.

Suggested Topics:

1. **RSA Cryptography**: How do you send your credit card number over the internet so that Ebay can see it but Comcast (or someone snooping on your network) can't? Is there a way to encrypt your data without knowing how to decrypt it? More importantly, what about number theory and groups tells us we can do this.

2. **Coding Theory**: When you transmit a message, it is reasonable to expect the introduction of some errors. Is there a way to "pad" your message so that even if some of it can be lost (or randomly altered), you can still reconstruct the original message? What is more efficient than just sending the message 10 times? And how do polynomials help us in this process?

3. **Knot Theory and Braids**: Knot theory studies the different ways a rope or ropes could be tangled up. How can you tell different knots apart? We would consider the much simpler question of understanding braids (which can be transformed into knots) using group theory. This is one example of a larger topic: group representations.

4. **Lattices and Boolean Algebra**: Rings are sets with two operations. When studying sets, you might also consider the operations of *union* and *intersection*. Are these like plus and times for rings? Or are there other axioms that govern how this operations work? Boolean algebras are a generalization of the set (or logic) operations, and provide the basis for the algebra of electrical circuits. Besides the application, this is a nice example of other algebraic structures beyond groups and rings.

5. **Wallpaper Groups**: How many different wallpaper patterns are there? What can abstract algebra tell us about translations, rotations, mirrors, and other symmetries? Oh, and crystals!

6. **15 Puzzle**: This physical puzzle consists of 15 squares tiles that can slide around a 4 by 4 grid (so one open space that an adjacent tile can slide into). Here's the question: if the tiles fell out and you randomly put the grid, what is the probability that you would be able to slide them back into their correct position? How can groups help us some the puzzles that have a solution?

7. **Rubik's Cubes**: How can groups help us solve a Rubik's cube? This will serve as an excuse to investigate some interesting ideas in group theory. Plus: learn to solve a Rubik's cube!

8. **Combinatorics - Counting bracelets**: How many different bracelets can you make using 10 beads that come in 4 different colors? Careful: two bracelets are the same if it is possible to flip or rotate them to line up the colors. How many different ways can you paint to faces of a cube using 3 colors? We will see that groups of symmetries help us answer these questions. Along the way we will explore *group actions* and *orbits* and *stabilizers*.

9. **Cayley Graphs**: Here is another interesting connection between algebra and combinatorics, this time dealing with graph theory. For any group, we can define a graph that describes how that group "acts" on itself. Given any graph, we can ask what the group of symmetries (really automorphisms) are. There is lots to explore here, including lots of pretty pictures.

10. **Free Groups and Representations**: We have seen that groups that look different might end up being the same (i.e., isomorphic). What are some interesting ways to represent groups that might help classify them? A *free group* is the group you get using some number of letters and considering all possible strings of these letters (and their inverses). This is an infinite group, so how does it help us describe finite groups? Quotients! And then a very interesting question: how hard is it to determine whether two groups are the same?

11. **Classifying groups with direct and semi-direct products**: Another way to classify groups is to represent them in terms of smaller groups. For example, we can represent $\mathbb{Z}_6$ as $\mathbb{Z}_2 \times \mathbb{Z}_3$, which has the benefit that the indices are prime numbers. Can every group be represented this way? Uniquely? Of course $\mathbb{Z}_m \times \mathbb{Z}_n$ and similar are always abelian, so we will need something else for non-abelian groups.

12. **Algebraic Number Theory**: A *Diophantine equation* is a polynomial equation whose solutions are supposed to be integers. A classic example is the equation $x^2 + y^2 = z^2$, where solutions are Pythagorean triples. The quest to solve Diophantine equations historically led to the development of one half of abstract algebra: rings and ideals. The idea is to use these abstract algebraic objects to help us understand regular numbers.

13. **Symmetric Polynomials**: The other half of abstract algebra (group theory) grew out of the study of *symmetric polynomials*: polynomials in multiple variables such that if any of the variables are interchanged, one obtains the same polynomial. What is so special about these polynomials, and how can studying them help us understand regular polynomials? How might we describe these polynomials in simpler terms?

14. **Category Theory**: We have seen that groups and rings both have homomorphisms, and that these behave mostly the same way. In linear algebra, you have linear transformations that also satisfy a sort of homomorphism property, and they also have kernels! Category theory is an attempt to generalize and abstract our already general, abstract mathematical structures. What are the rules that govern how all these structures and functions between structures behave?

15. **Ordered Structures**: Groups and rings for us have been sets with two operations. But many of our favorite examples, like the integers, rational numbers and real numbers have another property: the elements are *ordered*. How might we describe a general theory of *ordered* groups, rings, and fields? Can every field be ordered? Can ordered groups or fields have "infinite" elements? Yes! But what does that mean?

About the project:

You will work in groups of 2-3 students to investigate one of the topics described above. This investigation will be a mix of answering specific questions that I provide you, and doing general background research on the topic. This work will result in both an oral presentation and a paper.

The presentation will consist of 20 minute talk/lesson on your chosen topic. The paper should be roughly 10 pages typed (including pictures), but the actual length should be based on the content (some topics might require more or less writing).

Along the way, lots of help will be provided. Some class time during the final week will be available, but you will need to find time outside of class to work on this as well. Everything will be due at our Final Exam period (Tuesday, May 5th at 1:30pm), when you will give your talk, turn in your paper (and turn in the take-home final exam).