MATH 101 - SETS, GROUPS, AND TOPOLOGY
INFORMATION ON THE FINAL PROJECT

What? The final project is an opportunity for you to follow your curiosity and connect the mathematics we have been learning with your broader interests and coursework. Part of the goal is to show you the range of applications and connections of modern mathematics to other fields, but the project also gives you the chance to explore a related mathematical topic more deeply. We hope you will enjoy exploring and synthesizing some mathematical topics. The project is to be done in groups of 3; because 3 does not divide the number of students in the course, we'll have one group of 2; if you'd like to be that group of 2, please email me – first come, first serve.
Your group will learn about a topic and write an 8-12 page exposition of your topic. Your report should include a clear introduction that motivates your topic and sets the stage for the rest of the report. We expect to see serious mathematical content, including definitions, theorems, and proofs. The report should also *cite* all the references that you used.
You should typeset your project (preferably with latex, but this is not required). You should also submit a paragraph detailing each group member's contributions to the overall project.
The rest of this handout gives the key deadlines, the grading rubric and presents some potential project ideas. If there's some other topic you're interested in writing about, you are more than welcome to. I highly recommend talking with me, Grace, or Michele (and ideally more than one of us!) about project ideas.
When? Below are the key dates:

- Monday, October 29: *Project proposal due* (this will part of assignment 13). Your proposal should include your group members, your topic, and a rough outline of your project (about a page). This outline should address the following questions:
  - What are your main motivating questions or problems?
  - What sources do you plan to read?
  - What theorems will you prove?
- Tuesday, November 20: *Project draft due.*

Date: October 18, 2018.

- Friday, November 30: *Peer review due.* You will have to read somebody else's draft, give feedback, and suggest improvements (about a page is enough).
- Friday, December 7: *Final project due.*

How will this be graded?
The final project will be graded out of 100 points (the breakdown is below), and will count for 10% of your final grade.

- Draft is turned in on time and is reasonably complete (10 points).
- Peer review contains valuable feedback (5 points).
- Draft feedback was incorporated (5 points)
- Motivation and Introduction (10 points):
  - Discussion of why the topics are interesting.
  - Clear connections with course topics.
  - Clear motivating questions.
  - How does this fit in the bigger picture?
- Communication and Writing Style (15 points)
  - Ideas are clearly communicated.
  - Correct grammar and spelling, good mathematical writing (for example, using precise language)
  - Is the paper readable? Are there clear transitions between topics?
  - Material is explained at the level of a 101 student.
- Definitions (10 points):
  - Clear, correct, and precise mathematical definitions.
- Examples (10 points):
  - Examples are correct, complete and well-chosen.
  - There are sufficient examples to help the reader understand key definitions, theorems, and proofs.
- Mathematics (20 points):
  - Clear statements of theorems/propositions/lemmas/corollaries/etc.
  - Correct and consistent use of notation.
  - Complicated proofs are broken up into smaller pieces.
  - Correct and concise mathematical proofs.
  - Content and techniques are at the level a 101 student would understand.
  - Arguments are complete, and details are provided.
- Bibliography (5 points):
  - Citations are correct and complete.
  - Citations come from reputable sources.
- Overall cohesiveness (10 points):
  - The topics are in a logical order.

- The topics fit together into a coherent story or theme.
- Each group member's project contributions are documented.

Some ideas of projects

Some of the topics below are covered in the course textbooks. Many are not: Wikipedia or google are your best tools to quickly find an overview and links to further references. Feel free to ask me if you need suggestions for references. As said above, these are only suggestions, but if you would like to do a completely different topic I highly recommend talking to me and/or one of the CAs first.

Projects on group theory (and connections with the rest of math).

- More on the symmetric group: the symmetric group S_n has an interesting normal subgroup called A_n (the alternating group): you could explore its definition and properties. You could also look at why any permutation can be written as a product of certain simple permutations, called cycles, or why any finite group is isomorphic to a subgroup of a symmetric group.
- Group actions: in some sense, the group of symmetries of an equilateral triangle "acts" on the equilateral triangle itself (by rotating or reflecting it). How can we make this idea precise and generalize it?
- Ring theory and/or field theory: a ring is a set with *two* operations, an addition and a multiplication, satisfying certain properties. The set forms an abelian group under addition, but not necessarily under multiplication (inverses are lacking). There is a *distributive law* that says multiplication plays well with addition. An example is the set of integers with the usual addition and multiplication. A *field* is a special kind of ring, where the multiplication has inverses except for 0. An example is the reals with the usual addition and multiplication.
- Free groups and presentations: we looked (or will soon look) at cyclic groups: group that are generated by just one element. We also saw for example that D_n is generated by two elements, r (a rotation), and s (a reflection), and that these elements satisfy certain properties, such as $r^n = e$, $s^2 = e$ and $rs = sr^{-1}$. It turns out these properties characterize D_n. Even more, *any* group can be written as generated by a bunch of generators satisfying some properties.
- The Sylow theorems: this is a collection of small theorems about the order of certain subgroups of finite groups. Specifically, if

for a prime p, n is maximal such that p^n divides the order of G, then G has a subgroup of order p^n. This has applications to classifying finite groups of a given order. For example: what are all the possible groups with six elements?

- The classification of finite abelian groups: there is a theorem that says that any finite abelian group can be written as a product of cyclic groups, in a way that is, in some sense, unique. You could explore the proof of this theorem.
- Simple groups: Simple groups are those that do not have a proper normal subgroup. The Jordan-Hölder theorem says that any finite group can be in a sense decomposed into its simple subgroups. Examples of simple group include some "nice" groups, like what is called the alternating group, but also some "ugly" groups that defy understanding, including a *monster* group of order approximately $8 \cdot 10^{53}$...
- Properties of the group of units: recall that $U(n)$ is the group of elements in $\mathbb{Z}_n$ that have a multiplicative inverse. What is the order of $U(n)$? When is $U(n)$ cyclic?
- Elliptic curves: these are ("non-singular") curves of the form $y = x^3 + ax + b$. It turns out one can define a group operation on an elliptic curve, given by $x * y =$ the other point z on the line segment from x to y (if $x = y$, we take the line tangent to the curve). See the wikipedia page for pictures! Checking it is a group is not obvious (even for associativity!). The group is connected to several topics, including:
  - Elliptic curve cryptography.
  - Fermat's last theorem: no natural numbers a, b, c satisfy $a^n + b^n = c^n$ for $n \geq 3$.
  - The congruent number problem: which rational numbers can be the area of a right-angle triangle with rational sides?
- Unsolvability of the quintic: there are no closed form general formula giving the roots of a polynomial of degree 5.

Projects on applications of group theory outside of math.

- RSA encryption: used everywhere on the internet.
- Group theory and the Rubik's cube: Study the group of moves of the Rubik's cube, and think about how it can help understand the cube.
- Group theory in music.
- Group theory in physics.
- Group theory in chemistry.

Projects on other fields of math.

- Boolean algebras: these are in a sense a common generalization of sets and logical propositions. They have applications to logic and computer science.
- Algebraic, irrationals, and transcendental numbers: explore these different types of real numbers. Prove that numbers such as e or π are irrationals.
- More on number theory:
  - The fundamental theorem of arithmetic says not only that a natural number is a product of primes (proven in class), but that this product is (up to permutation) *unique*. How is this proven? What are interesting generalizations and applications?
  - What is the Euclidean algorithm? What can we do with it?
  - Primality testing: given a number, how do we check (quickly) that it is prime?
  - Types of primes: Fermat primes, Mersenne primes, etc.
  - Lagrange's four squares theorem: Every natural number is a sum of four non-negative squares! For example, $1 = 1^2 + 0^2 + 0^2 + 0^2$, or $310 = 17^2 + 4^2 + 2^2 + 1$.
- More on infinite sizes and set theory: there are many more topics:
  - Explore *orderings* and *ordinal numbers*, that allow you to count past the finite numbers.
  - Prove the Cantor-Schröder-Bernstein theorem, that says that cardinalities of sets are linearly ordered.
  - Think about the *continuum hypothesis*: every uncountable subset of reals is in bijection with the reals.
  - What is the *axiom of choice* and how can it allow you to get more than you started with (the Banach-Tarski paradox – also connected with group theory)?
- The Cantor set: this is the set of real numbers expressible in base 3 using only the digits 0 and 2. This is a "fractal" set with very interesting properties.
- Graph theory: this is a field of math by itself, with applications (for example) in computer science. Topics include:
  - The four color theorem: the countries of any map can be colored using just four colors, in such a way that no two countries with the same color share a border. Any known proof of this result uses a computer!

  - Ramsey's theorem: At a party with six students, there are three that either are all strangers or are all friends. This can be generalized to parties with any number of students.
  - The coloring number of the plane: how many colors do you need to color the plane in such a way that no two points at distance exactly one have the same color? (A biologist at MIT recently made a breakthrough on this!)
  - The seven bridges of Königsberg: how do you tour a city while making sure to cross all its bridges exactly once?
  - The art gallery problem: how many people do you need to guard an art gallery?
- Constructing the real numbers: similarly to how groups were defined, one can define the real numbers to be a set satisfying a certain list of axioms, and then check that there really is a set satisfying those axioms. One construction looks at equivalence classes of Cauchy sequence, another goes via what is called Dedekind cuts of rational numbers.
- Constructibility of the n-gon: for which values of n can you construct an n-gon with just straight edge and compass? The answer is given by the Gauss-Wantzel theorem: exactly for the n's that are a power of 2 multiplied by a product of Fermat primes...
- The pigeonhole principle: if we put k pigeons in n boxes and $k > n$, we must have a box with more than one pigeon... How can that intuitively obvious statement help us prove interesting things?