Math 561/661 **Fall 2023**
Writing Topics **Drew Armstrong**

This course has an optional writing credit.

Details.

- Write a paper on a topic that is closely related to the course material.
- The style should be similar to a typical math textbook or research paper.
- The paper should be typeset instead of hand written.
- The paper should be approximately 10 pages long. Of course this will include white space because typeset mathematical formulas always need white space.
- The paper should include a series of small results and definitions, leading up to the proof of an interesting theorem. The definitions, statements and proofs should be written clearly and correctly.
- The paper should include an introduction/abstract and bibliography.
- The first draft must be submitted by **Thurs Oct 12**. I will provide feedback and then you must submit a final version incorporating this feedback. The final due date is **Wed Dec 13**.
- I will be happy to set up Zoom appointments to discuss possible topics.

Some Possible Topics.

- **The 5/8 Theorem.** Let G be a finite group and let $P(G)$ be the probability that two random elements $a, b \in G$ satisfy $ab = ba$. The "5/8 Theorem" says that
$$P(G) > 5/8 \quad \Rightarrow \quad P(G) = 1.$$
Equivalently, if G is a non-abelian group then the probability that two random elements commute is less than or equal to 5/8. Prove it.

- **Wallpaper Groups.** Let $\text{Isom}(\mathbb{R}^2)$ be the group of isometries $\mathbb{R}^2 \to \mathbb{R}^2$. We say that a subgroup $G \subseteq \text{Isom}(\mathbb{R}^2)$ is "discrete" if there exists some real number $\epsilon > 0$ such that the distance between $g(\mathbf{x})$ and $\mathbf{x}$ is greater than ϵ for all $g \in G$ and $\mathbf{x} \in \mathbb{R}^2$. It turns out that there are only 17 such groups! Describe the classification and prove at least some of it.

- **Polyhedral Groups.** Let G be a finite subgroup of $SO(3)$. Then G is either (1) a cyclic group C_n, (2) a dihedral group D_{2n}, (3) the group T of rotations of a tetrahedron, (4) the group O of rotations of an octahedron/cube, or (5) the group I of rotations of an icosahedron/dodecahedron. There are no other possibilities. Give a proof.

- **Fermat-Euler-RSA.** Discuss Fermat's Little Theorem, Euler's Theorem, and the following slight generalization: Let p and q be distinct primes. Then for all integers $a \in \mathbb{Z}$ we have
$$a^{(p-1)(q-1)+1} = a \mod pq.$$
Prove this theorem and explain how it is the basis of the RSA cryposystem.

- **Sylow Theorems.** Let G be a finite group with $\#G = p^\alpha m$ where p is prime and $p \nmid m$. Then (1) There exists a subgroup of size p^α, (2) Any two subgroups of size p^α are conjugate, and (3) the number of such subgroups (called *Sylow subgroups*) is congruent to 1 mod p. Prove one or more of these theorems.

- **The Gaussian Coefficients.** The q-binomial theorem says that
$$(a+b)(a+qb)\cdots(a+q^{n-1}b) = \sum_{k=0}^{n-1} q^{k(k-1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q a^k b^{n-k},$$
where $\begin{bmatrix} n \\ k \end{bmatrix}_q$ are called the Gaussian or q-binomial coefficients. Give an introduction to these numbers and prove at least one interesting theorem about them.

- **The Cartan-Dieudonné Theorem.** A reflection matrix F satisfies $F^T = F$ and $F^2 = I$. Show that every matrix in the group $O_n(\mathbb{R})$ can be expressed as a product of at most n reflections. One consequence is that every non-identity matrix in the group $SO_3(\mathbb{R})$ is a product exactly two reflections, i.e., is a rotation.

- **Burnside's Lemma.** This is a formula for counting finite structures up to symmetry. For example, it can be used to prove that there are 57 different ways to color the 6 faces of a cube using 3 possible colors, up to rotational symmetry. Prove this theorem and give some interesting examples.

- **Quaternions.** The ring of quaternions is a generalization of complex numbers. It is the set of expressions of the form $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ where a, b, c, d are real numbers and the symbols $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ satisfy certain relations, such as $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}$. Describe the basic theory of this ring and explain how it can be used to encode rotations in three dimensional space.