Project: Explorations with Groups and Numbers

MME 529 Project Ideas

William J. Martin, WPI

Instructions: *Here are some suggestions for group projects to be presented on May 30th. Groups should consist of 2-3 students. Oral presentations should be efficient (jam-packed with mathematics) and about 20 minutes in length. Each team should accompany this with a written report of at most 20 pages in length.*

Feel free to suggest an entirely different project if a good idea comes to you!

- Multiplicative Functions: What lessons can your students learn from the study of arithmetic functions such as ν, σ, ϕ and μ?

- Check digits for error detection: Gallian discusses check sums for USPS money orders, UPC codes, etc. The project will also compare ISBN-10 versus ISBN-13, check digits for credit card numbers, and more.

- Subgroups of $\mathbb{Z}_n$: Work out the full lattice of subgroups of the group of integers modulo n. This will depend on n. Put the trivial subgroup $\{0\}$ at the bottom, the full group $\mathbb{Z}_n$ at the top, and draw a segment from H to K when H is a subgroup of K for each H and K in the diagram.

- Matrix groups: Over any field $\mathbb{F}$ — such as the real numbers, complex numbers, rational numbers, integers modulo a prime — the square $n \times n$ invertible matrices form a group called the "general linear group". This group is fundamentally connected to symmetries of space, to elementary row operations, and more. This project explores this group $\mathrm{GL}(n, \mathbb{F})$ and other matrix groups such as the special linear group $\mathrm{SL}(n, \mathbb{F})$, the orthogonal group (consisting of real matrices whose inverse is equal to their transpose) and the unitary group (consisting of complex $n \times n$ matrices whose conjugate transpose is equal to their inverse).

- The Rubik's Cube Group: Suppose G is a group generated by some small set of elements $g_1, g_2, \ldots$. The "word problem" in group G involves factoring an arbitrary element of the group into generators; i.e., given $h \in G$, we want to express h as a product of generators — say, for example, $h = g_3 \cdot g_1^{-1} \cdot g_3 \cdot g_1 \cdot g_2^2$ — hopefully in the most efficient way. A very popular example of this problem is the Rubik's cube puzzle where the generators are six basic rotations and the group has size roughly 43×10^{18}.

- The kernels of abstraction: How do we get students to understand the power of abstraction? How do we help them see common features among very different-looking things?

- Orders of elements in symmetric groups: Consider S_n, the symmetric group on n letters. An *involution* is an element of order two: $g \neq e$ yet $g^2 = e$. How many involutions are there in S_n? How many elements have order three? four? What is the largest possible order for an element in S_n?

- Symmetry in Art: What groups arise in painting and sculpture? What about music? Find examples where the artist knowingly exploits interesting forms of symmetry.

- ElGamal encryption: We discussed elliptic curve encryption in class, but the general strategy is valid in any finite group. Let G be a group and suppose our messages are elements of G. We assume g is a generator for G (so that $\langle g \rangle = G$) and Alice generates a secret integer k, computes $h = g^k$ in G, and publishes (G, g, h) while keeping k secret. Any user Bob who wishes to send an encrypted message $m \in G$ to Alice first generates a random integer ℓ and transmits $(g^\ell, m \cdot h^\ell)$. You can work out the decryption algorithm from here. The best example for G when we explore this system is to take the multiplicative group of a finite field, say $G = \mathbb{Z}_p^*$ where p is a large prime.

- Braid Groups: The braid group B_n on n strings is an important and fascinating example of an infinite group. The short note below by Daniel Glasscock explores some questions about B_n, but gets too deep into the mathematics too quickly for us. Nonetheless, the note is certain to inspire some questions that can be formed into a project. Here's the reference: `https://people.math.osu.edu/glasscock.4/braid_groups.pdf`

- Group Theory in Crystallography: This is a subject about which I know little. It is intuitively obvious that crystals have spacial symmetry and some very nice groups arise. But chemists and crystallographers apparently need much more detail about groups to fully understand the objects that they study. Here is one possible source of material for such a project: `http://www.math.ru.nl/~souvi/krist_09/cryst.pdf`