MA 294: Applied Abstract Algebra / Spring 2022
Optional projects
Due last day of class
(plan of action due 12 April)

What.

If you would like, you may do an optional project for this class. This project may be a short paper (3–5 pages), one that demonstrates some grappling with math related to algebra in some way. Or it may be something more creative, perhaps something you'd want to share with the class — a play, a video, a poster, a piece of art. If you do a creative project, you may need to supplement with a shorter (1–3 pp.?) text that explains the connection with the mathematics, depending on how clear that is from the project. The project must show evidence of understanding and clearly explaining some abstract algebra.

- You must use at least two sources in good faith. Of course you must attribute all your sources! The exception is if you're really working out some mathematics by yourself; explain this as well.
- If you are writing a paper, it must be typed; it may not be handwritten!
- This optional project cannot hurt your final grade; it can only help it.

Dates.

- On Tuesday 12 April, you must turn in a written plan of action: What's your topic, what are you planning to do (if you're not writing a paper) and is this something you'll want to present to the class, what sources will you use, what's the connection with algebra (if not obvious).

- The final deadline for the project is the last day of class, Wednesday 4 May.

Ideas.

These are a few ideas for projects and how to get started. More may be added over the next few weeks. Some of these will require you to learn a little bit more on your own than others — come talk to me if you want to know more. Also feel free to suggest your own ideas — please check in with me about the algebra connections.

Prof. Keith Conrad of UConn has a written a number of mathematical blurbs that may give you more ideas.

- **Games.** Each of these games relies on some underlying mathematics; in addition to describing this, you should also answer some kind of question about the game using algebra.
  1. The Fifteen Puzzle: See, for example, Exercise 12.7.19 and Prof. Keith Conrad's writeup.

  2. Spot It: See this MathOverflow post to get you started. You'll have to use a little bit about finite fields (section 22.3) and learn a bit about the projective plane (section 23.7).

(3) Set: See, for example, this writeup of Charlotte Chan for the underlying mathematics. You'll have to use finite fields (section 22.3) and learn a bit about abstract vector spaces (for example, chapter 20 of Judson).

(4) Rubik's cube: See Prof. Conrad's writeup to get you started.

- **History of math.**

(5) Galois and his work: Group theory dates back to the work of Evariste Galois, an early 19th century French mathematician and political activist who died in a duel in his early twenties. Write a short biography of his life and explain how his work connects to group theory in our modern conception.

- **Math education.**

(6) Abstract algebra for kids: Develop several lesson plans for elementary or middle or high-school students introducing them to some of the ideas of abstract algebra in a hands-on way. Possibly this book by Natasha Rozhkovskaya on ideas of the Berkeley math circle, or others like it, may be good sources.

- **Art.**

(7) Escher's *Print Gallery* and the Droste effect: See de Smit and Lenstra's paper in the Notices of the AMS, or Prof. Conrad's retelling. You'll have to learn a little bit about quotient groups.

- **Geometry.** Connections to robotics here via the study of the group SO(3)[1]

(8) Classification of finite rotation groups: Every finite symmetry group of an object in 3 dimensions is either cyclic, dihedral, A_4, S_4, or A_5. See Exercises 21.7.19–21 or section 5.9 of Artin's *Algebra*.

(9) SO(3) and quaternions... more coming / come talk to me.

(10) Orbit recovery problems: see, for example `https://arxiv.org/pdf/1712.10163.pdf`.

For more connections between group theory and robotics/computer vision, take a look at this course syllabus of Prof. Yanxi LIU of Carnegie-Melon.

- **Combinatorics.** Many many more possibilities here; contact me.

(11) Pólya's theorem (Theorem 27.6), related to Burnside's lemma (Theorem 21.4).

- **Further in our textbook.**

[1] Tip of the hat to Dr. Edgar Costa for some of the references here.

(12) Error-correcting codes: Chapter 24. It's not looking likely that we'll get to this substantively in class.

- **Pure algebra.**

(13) Homomorphisms, quotient groups, and the first isomorphism theorem: A map $f : G \to H$ between groups is a *homomorphism* if $f(ab) = f(a)f(b)$ for every $a, b \in G$. The *kernel* $\ker f \subseteq G$ of a homomorphism is the preimage of the identity: $\ker f := \{a \in G : f(a) = 1\}$. The *image* of a homomorphism is what is sounds like: $\operatorname{im} f := f(G) \subseteq H$. The kernel is a subgroup of G, and f is injective if and only if $\ker f$ is trivial. The image is a subgroup of H (and f is surjective if and only if $\operatorname{im} f = H$). Moreover, if $K = \ker f$, then the left coset G/K of K in G are the same as the right cosets $K\backslash G$ of K in G (that is, K is what's called a *normal subgroup*), and the set of cosets G/K forms a group its own right with multiplication $(g_1K)(g_2K) = g_1g_2K$, the *quotient group* of G by K. The point of all this here is the completely natural isomorphism

$$G/\ker f \cong \operatorname{im} f$$

induced by f. This is the *first isomorphism theorem*. Any abstract algebra text is fine; for example, Judson sections 10.1, 11.1, and 11.2.

(14) Cauchy's theorem and the Sylow theorems: Cauchy's theorem tells us that a group of order divisible by a prime p must have an element of order p. The Sylow theorems vastly generalize Cauchy's theorem to precisely describe the maximal p-power subgroups of a finite group whose order is divisible by p. For example, S_4 has order 24, so that the highest power of 2 dividing $|S_4|$ is 8. The copies of $\mathrm{Symm}(\square)$ that one can find in S_4, which all have order 8, are the 2-Sylow subgroups of S_4. See, for example, Prof. Conrad's writeup.

- **Number theory.**

(15) Unique factorization in the Gaussian integers: In $\mathbb{Z}$ we have the following chain of reasoning:

$$\begin{aligned} \text{division algorithm (Theorem 8.3)} &\implies \text{Bézout's lemma (Theorem 8.4)} \\ &\implies \text{fundamental lemma (Theorem 8.6.1)} \\ &\implies \text{unique factorization into primes (Theorem 8.6.2)} \end{aligned}$$

Prove division algorithm in the *Gaussian integers* $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ and follow the chain of reasoning to prove unique factorization into primes in the Gaussian integers. (It's a little nicer to use the integer-valued *norm* $N(a + bi) = a^2 + b^2$ of a Gaussian integer $a + bi$ in place of absolute value; this norm is still multiplicative, so that a Gaussian integer α is in $\mathbb{Z}[i]^\times$ if and only if its norm is 1. The elements of $\mathbb{Z}[i]^\times$ are the *units*; they're what you ignore when you prove unique factorization.)

Can you do the same for $\mathbb{Z}[\sqrt{-2}]$? $\mathbb{Z}[\sqrt{-3}]$? Note that in the latter we have $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Is that a problem?

(16) Cyclicity of $\mathbb{Z}_m^\times$: Explain exactly for which m is the group $\mathbb{Z}_m^\times$ cyclic. See (7)–(9) on this problem set from MA 541 in Fall 2021 or many other sources.

- **Cryptography[2]:** You may (probably will) need to know about finite fields (section 22.3). You may need to know the RSA public-key encryption algorithm as background: see, for example, Chapter 7 of Judson. Apart from elliptic curve cryptography, these are topics I am personally not familiar with at all; you'll have to explain everything.

(17) Elliptic curve cryptography: Like RSA, but with an elliptic curve over a finite field replacing $\mathbb{Z}_m^\times$.

(18) Shamir's secret sharing and application, by BGW, to secure multiparty computation. Good reference: https://eprint.iacr.org/2011/136.pdf.

(19) Algebraic Manipulation Detection (AMD) codes: Possible reference: https://eprint.iacr.org/2008/030.pdf

(20) Blum and Micali prove that if discrete log is hard, then it's hard to figure out whether $x > p/2$ given $g^x \pmod{p}$; see Section 3.3 of https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Pseudo%20Randomness/How_To_Generate_Cryptographically_Strong_Sequences_Of_Pseudo-Random_Bits.pdf.

(21) Efficient proofs that $y = x^{2^t}$ for some suitably large t in a group of unknown order (like the RSA group). The goal is for verification to be much more efficient than the computation itself. References: https://eprint.iacr.org/2018/623.pdf and https://eprint.iacr.org/2018/627.pdf.

(22) Advanced Encryption Standard (AES)...

(23) Lattice-based cryptography...

[2] Thanks to Prof. Reyzin for most of the suggestions here.