MA 542: Applied Abstract Algebra / Spring 2023
Optional projects
Due 3 May last day of class
(plan of action due 14 April)

What.

If you have further to go, you may choose to do an optional project for this class. This project would typically be a short paper (3–5 pages), one that demonstrates some grappling with math related to ring theory, field theory, or Galois theory in some way. A more creative form is also possible; stop by to discuss.

- 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.
- Papers must be typed, not handwritten! If you're thinking about math or CS long-term, this might be a good time to get started with LaTeX.
- Of course, this optional project cannot hurt your final grade; it can only help it.

Dates.

- On April 14 turn in a written plan of action: What's your topic, what are you planning to do, what sources will you use, what's the connection with the course material (if not obvious).
- The deadline for the project is the last day of class, Wednesday 3 May.
- Perhaps you might be interested in presenting your project to the class? That would be during the last two class meetings of the semester, Monday 1 May or Wednesday 3 May.

Topic ideas.

These are a few ideas for projects and how to get started. Feel free to come and chat about topics with me or suggest your own.

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

- **Games.** Each of these games relies on some underlying linear (or projective-linear) algebra over finite fields; in addition to describing this, you should also answer some kind of question about the game using algebra.
  (1) Spot It: See this MathOverflow post to get you started. You'll have to learn a bit about the projective plane.
  (2) Set: See, for example, this writeup of Charlotte Chan for the underlying mathematics (uses vector spaces over finite fields).
  (3) EvenQuads: New game, similar spirit to Set, recently invented by Prof. Lauren Rose of Bard College and her student Jeffrey Perreira. See rules on the AWM website, and Arxiv paper by Rose and students analyzing some aspects of the game.

- **Art.**

  (4) 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. Mathematically more appropriate for MA 541 (it only uses some quotient groups), but it's a really cool topic. The paper is worth reading even if you don't choose to do this project, or any project.

- **Geometry.**

  (5) 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, for example, section 5.9 of Artin's *Algebra*. This is also more appropriate for MA 541, but it's also a really lovely topic!

- **Set theory.**

  (6) Zorn's lemma in algebra: See optional problems on HW # 5 to start. There are many other arguments that need Zorn's lemma, most notably various constructions of algebraic closures and extension theorems embedding algebraic extensions of K in algebraically closed extensions of K.

- **Algebraic geometry.**

  (7) Zariski topology on the prime spectrum of a ring: Let A be a commutative ring. The set of prime ideals of A can be endowed with a topology called the *Zariski topology* in which we call the subset of prime ideals that contain a fixed ideal of A *closed*. With this topology ring homomorphisms $A \to B$ induce continuous maps $\operatorname{Spec} B \to \operatorname{Spec} A$. For a possible sequence of exercises, see (5) on 2020 MA 741 HW #5 and (4) on 2020 MA 741 HW #6. (Or here's a similar sequence from Prof. Jay Shapiro of George Mason.) For a capstone, draw the topological space $\operatorname{Spec} \mathbb{Z}[x]$ as best you can.

  If you have further to go, the topological space $\operatorname{Spec} A$ may be enriched with a *sheaf* of rings making it into a *locally ringed space*, and these then may be glued together in appropriate ways to make *schemes*, which are the basic objects of study in modern algebraic geometry. See Hartshorne, *Algebraic Geometry*, II.1–2; Vakil, *The Rising Sea: Foundations of Algebraic Geometry*, Chapters 1–3; Eisenbud and Harris, *The Geometry of Schemes*.

- **Classical applications of field theory and Galois theory.**

  (8) Constructible numbers: Using field theory to answer classical problems studied by the Greeks — squaring the circle, angle trisection, doubling the cube, etc. See BB section 6.3; Dummit and Foote section 13.3; and others.

(9) Solving by radicals, insolvability of the quintic: We aim to cover some of this topic in class, but likely not in gory detail. Review solvable groups in BB chapter 7 and then see BB section 8.4. Also see 14.7 of Dummit and Foote.

- **Cryptography.**

(10) Error-correcting codes: Hamming codes, BCH codes, others? Uses arithmetic in finite fields, usually in characteristic 2. See, for example, Chapter 25 of Childs, A Concrete Introduction to Higher Algebra.

- **Number theory.**

(11) Gaussian integers, the two-square theorem, and generalizations: Prove division algorithm in the *Gaussian integers* $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$, (both algebraically and geometrically?), and follow the chain of reasoning to prove unique factorization into primes in the Gaussian integers. Then use arithmetic in $\mathbb{Z}[i]$ to prove the two-square theorem.

Can you do the same for $\mathbb{Z}[\sqrt{-2}]$? $\mathbb{Z}[\sqrt{-3}]$? $\mathbb{Z}[\sqrt{-5}]$? Note that $2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$ in $\mathbb{Z}[\sqrt{-3}]$ and that $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. Do these cause problems? What can you conclude about solutions to $x^2+dy^2 = p$ for primes p and small values of d?

(12) Factorization of ideals in subrings of $\mathbb{Q}[\sqrt{d}]$: Generalization of above. Possible reference (spoiler alert!): Prof. Conrad on factoring in quadratic fields. In particular, although the rings of integers in these fields are not UFDs in general, they do have unique factorization into primes for *ideals*.

(13) Counting irreducible polynomials of degree n in $\mathbb{F}_q[x]$: Alternate existence proof for finite fields of any prime-power order. See, for example, BB section 6.6.

(14) Quadratic reciprocity: *Quadratic reciprocity*, conjectured by Euler and first proved by Gauss, expresses a precise and surprising relationship a prime p being a square modulo another prime q and q being a square mod p. For example, 23 is a square mod 13 because $6^2 = 36 \equiv 23 \mod 13$, but one can check that 3 is not a square modulo 7. (If you're not familiar with the statement, can you guess it from playing around with small primes?) There are many proofs of this statement; a couple of them use field theory. For one approach, using Gauss sums, see, for example BB section 6.7 or section 2.2 of J. Booher's expository note. For another, to understand which you'll have to learn a little bit about Frobenius elements in Galois groups, see section 2.1 of the same note.