

180 : Linear Algebra over Finite Fields
Prof. Monica Vazirani

Prerequisites: Mat 22A or Mat 67. Mat 108 strongly recommended.

Course Description:

Everything you learn to do with systems of equations, matrices, and vector spaces over \mathbf{R} can be done over a finite field \mathbf{F}_q . In other words, instead of the scalars being real numbers, the scalars now come from a finite set, for which addition and multiplication still make sense.

We can now count things like how many points are on a line or on a plane, and so we get interesting connections to combinatorics. There are some card games based on these ideas that we will investigate. There are also applications to cryptography and error correcting codes.

We will explain what finite fields are, redo the highlights of linear algebra in this new context, and hopefully see some of the interesting applications.

Textbook: There is not a set textbook. Some material may follow parts of Combinatorics of Symmetric Designs by Ionin and Shrikhande or parts of Discrete Mathematics by Biggs or other online resources.

Grading Scheme: A combination of class attendance/participation, homework, and/or final exam. Precise weights among these are yet to be determined.

Topics covered include: Defining a finite field F . Points, lines, and planes over F . General vector spaces over F . Matrices and linear transformations. Basis, dimension, and counting. Determinant and invertible matrices. Projective geometry over F . Constructing and understanding other finite fields. Applications such as codes, designs, Latin squares, games.